INSTANT MESSAGING

CHECKLIST

Version 1, Release 1.4

18 July 2008

Developed by DISA for the DoD

This page is intentionally blank.

TABLE OF CONTENTS

Page

This page is intentionally blank.

CHANGES

- IM0350 – Changed check procedures to verify warning banner contents are in compliance with the new DoD Warning Banner signed by the DoD CIO on 9 May 2008.
-

This page is intentionally blank.

1. VMS 6.1 INSTANT MESSAGING REVIEW PROCESS

1.1 Instant Messaging Checklist Use

There are many instant messaging platforms and protocols available. The instant messaging checklist should be used for **enterprise instant messaging systems**. These requirements do not apply to Managed Enterprise Services. Some of the more popular enterprise instant messaging systems include the following:

- IBM Lotus Instant Messaging
- Jabber XCP
- Infoworkspace
- Microsoft Live Communications Server
- Ipswitch Instant Messaging
- WiredRed e/Pop
- Effusia Business Messenger
- Sigaba Secure IM
- Sun One Instant Messaging

If it cannot be determined the instant messaging system is an enterprise instant messaging system, then research the product on the Internet or vendor's website. If it still cannot be determined, call the vendor and ask them directly.

***NOTE*:** Video teleconferencing is covered in the Video Tele-Conferencing STIG.

1.2 Requirements

The following section presents the data collection and analysis methodology for a Instant Messaging Security Readiness Review (SRR). The items reviewed as part of this SRR are based upon the requirements published by DoD Directive (DoDD) 8500.1, paragraph 4.18. The DoD Directive, DoDD 8500.1 requires guidelines to be developed by DISA FSO in accordance with DoD-approved security configuration as specified in the DoD Directive O-8530.1

The requirements to perform an Instant Messaging SRR are as follows:

- *Instant Messaging Security Technical Implementation Guide* – The Instant Messaging STIG will assist the reviewer with further detail in performing the instant messaging checks. The Instant Messaging STIG may be downloaded from the IASE web site located at http://iase.disa.mil.

- *Instant Messaging SRR Checklist* - A comprehensive list of checks that provide step-by-step procedures on performing an Instant Messaging SRR. The checklist may be downloaded from IASE web site located at http://iase.disa.mil.

- User access to the Vulnerability Management System (VMS) which is located at https://vms.disa.mil/VMSMain.asp

1.3 Data Collection

The initial data collection is achieved through the Instant Messaging SRR Checklist. The checklist provides procedures for evaluating instant messaging systems and their potential security vulnerabilities. Listed below are the general steps involved in performing an Instant Messaging SRR.

1. Prior to arriving onsite, acquire the latest printed copy of the Instant Messaging Checklist.
2. Ensure that you have a valid VMS account.
3. If possible, acquire a current copy of the sites instant messaging topology (network diagram) prior to arriving on site or obtain a copy as soon as possible after arriving on site.
4. During or soon after the in-brief at the site, obtain the names and phone numbers of the onsite POCs for the instant messaging review.

1.4 Assessment Procedures

The reviewer is responsible for coordinating with site personnel in arranging the review of the site’s network. Listed below are the procedures for the collection of SRR data:

1. Interview the Instant Messaging Administrators/IAOs, either individually or as a group, to complete the Instant Messaging SRR Architecture and Policy (Non-computing) and Instant Messaging Computing checks.

2. The Team Lead will create a Vulnerability Management System (VMS) Visits folder and provide the visit names to the reviewer.

3. After all of the data for the Instant Messaging SRR is collected and the Instant Messaging Checklist is complete, then enter the information into VMS.

4. Enter the Instant Messaging SRR results into the proper VMS visit by cross referencing the Vulnerability ID with the STIG ID located on the Instant Messaging SRR Checklist.

5. Upon the completion of entering the vulnerabilities into VMS, the reviewer will verify that no vulnerabilities are in the Not Reviewed (NR) status. Any Not Reviewed vulnerabilities will be reviewed again to ensure it has been entered correctly.

6. Open findings will be reviewed to ensure the “Finding Details” field has accurate text. If the “Finding Details” field is empty, the reviewer will enter appropriate text explaining the cause of the Open Finding.

7. A Severity Code can be downgraded to a lower category on an Open Finding only if DISA FSO Instant Messaging Checklist has provided documentation allowing that particular vulnerability to be downgraded. The downgraded finding will meet the allowable mitigations specified in the documentation. In addition, all downgraded vulnerabilities will contain a reason why it is being downgraded.

8. The reviewer will discuss with the site personnel the feasibility of closing all Category I findings before the team leaves the site. The reviewer will keep the Team Lead informed of all Category I findings and provide additional emphasis and clarity when explaining why some Category I findings cannot be closed immediately.

9. Floppy disks, CDs, data entry forms, and reports will be handled and protected in accordance with their level of classification.

10. The reviewer will communicate to the Team Lead the status of VMS data entry through the daily meetings and will send an email to the Team Lead only if the VMS data entry cannot be completed on site.

1.5 VMS Instant Messaging SRR Data Entry Procedures

1.5.1 Performing the Review

Verify the asset is registered in VMS under the correct organization. Assets not registered will need to be created. When creating the asset, the asset ownership defaults to the person creating the asset. It is recommended that the SA create the asset. If the reviewer creates the asset the permissions will need to be reassigned to the SA.

1. <u>Creating the Asset</u>

1. Expand Asset Findings Maintenance
2. Expand Assets/Findings
3. Expand Visits to display sub-folders. *(Reviewer Only) SA will expand Location.*
4. Expand the sub-folder assigned. Each subfolder represents individual visits in VMS assigned for review.
5. Expand the visit and display the location summaries for the visit. Within the location, assets are divided into computing, non-computing, and CNDS.

1.1 <u>Creating Non-computing asset</u>

1. Click the yellow folder icon located at the right of ‘Non-Computing’.
2. Click the General tab
3. Enter the Display name. The standard name for network non-computing asset will be: “SiteName_Instant_Messaging_Policy”
4. Verify “Location”
5. Verify “Owner”: Used to register asset to parent or child location.
6. Verify “Managed By”: Used for remote locations being managed.

7. Verify Mac level, Confidentiality, & Classification is correct.
8. Click the ‘Asset Posture’ tab to add functions to the asset
9. Expand Non-computing
10. Expand ‘Application’
11. Click ‘Instant Messaging Architecture and Policy’
12. Click ‘>>’ to move it to the ‘Selected’ window
13. Click the Systems / Enclaves tab
14. For registered enclaves, choose the correct enclave.
15. If the enclave is not present, ensure that the IAM or Team Lead works with the appropriate site personnel to request an enclave.
16. Click ‘Save’

1.2 Creating Computing asset

1. Click the Create Icon located next to computing. The asset form is displayed.
2. Click the General tab and enter the information into the required fields.
3. Click the asset identification tab and enter the IP address, MAC address and click add.
4. Click the Asset Posture Tab and drill down to select the following functions:
   - Operating System, Role, and Application – Generic Instant Messaging Application or whatever application you are reviewing.
5. Click the ‘>>’ to move it to the ‘Selected window
6. Click Save

2. Reassign Permissions for Asset (If Required)

1. Expand Permissions
2. Click Reviewer Asset Update
3. Select Visit and submit
4. Select Asset and submit
5. Select User and submit

3. Procedures for Review of the Asset

If all registration tasks have been accomplished, use the following procedures:

1. Expand Asset Findings Maintenance
2. Expand Assets/Findings
3. Expand Visits to display sub-folders. *(Reviewer Only) SA will expand Location.*
4. Expand the sub-folder assigned. Each subfolder represents individual visits in VMS assigned for review.
5. Expand the visit and display the location summaries. Within the location, assets are divided into computing, non-computing, and CNDS.
6. Expand ‘Non-Computing’ and ‘Computing’.
7. Expand ‘Must Review’ *(Reviewer Only) SA will not see ‘Must Review’*. If an asset was just created it would reside in ‘Not elected for Review’ section. Have the Team Lead move the asset to ‘Must Review’.

8. Expand Asset to review. Ready to review is colored in RED Note: When you drill down into the asset you will find Vulnerabilities assigned to the Instant Messaging component and IAVMs when the OS is expanded.
9. Expand the instant messaging component and each Vulnerability Key.
10. Update the 'Status' of the vulnerability
11. Identify details on all open vulnerabilities
12. System Administrators will need to update the POA&M prior to saving.
13. System Administrators should expand the OS assigned to the asset and each IAVM. Verify the OS level meets the required release or patch level. Asset must be in the same status such as 'Open'
14. Save the updates to the asset.

4. <u>Verify that all necessary assets were reviewed</u>

1. Select Asset Findings Maintenance
2. Expand Assets/Findings
3. Expand visits to display the sub-folders
4. Expand the sub-folder assigned
5. Expand the visit and display the location summaries. Within the location, assets are divided into computing, non-computing, and CNDS
6. Expand 'non-computing'.
7. Expand 'Computing'
8. Expand 'Must Review' (If checkmarks are gone, the asset has been reviewed.)

5. <u>Add Comments</u>

1. Select Visit Maintenance
2. Expand Organization for the visit.
3. Expand Visit
4. Locate the visit.
5. Click on CCSD or enclave name.
6. Comments Tab – Add comment
7. Save Changes

6. <u>Compliance Monitoring</u>

1. Select Reports
2. VC06 – Asset Compliance Report
3. Can select an asset or an org
4. Select "open" status
5. Can sort on different fields
6. Display (Finding Comments, Finding Long Name, Finding Details, Vulnerability Discussion)
7. The AS01 report assists the reviewer or SA by quickly identifying the assets at the location the review is being performed. In the section "Looking at Network Assets" is a quick step by step instruction in creating the report. The site may want to do other

reports, if your site manages or owns assets, which are not located at the site. Check Child Locations if applicable. Navigate to the Reports menu, Select the AS01 Report, and select the desired criteria for the report.

8. The VL03 report assists the reviewer or SA by quickly identifying the IAVMs that will be identified to the asset when you select the operating system of the asset. Navigate to the Reports Menu, Select the VL03 Report, and select the desired criteria for the report.

2. INSTANT MESSAGING CHECKLIST

2.1 Instant Messaging Architectures

IM0010: No policy prohibiting peer-to-peer applications or software exists

Vulnerability Key: V0015437

STIG ID: IM0010

Vulnerability: No policy exists that prohibits peer-to-peer applications or software.

IA Controls: ECSC-1 Security Configuration Guidance

Categories: 12.4 CM Process

Responsibility: Information Assurance Officer / System Administrator

References: Instant Messaging STIG

Severity: Category III

Vulnerability Discussion:
Pure P2P networks operate with peers acting as equals and merge the roles of clients and server. Pure P2P has no central server managing the network. Hybrid P2P has a central server that keeps information on peers and responds to requests for that information. Peers are responsible for hosting available resources and for letting the central server know what resources they want to share, and for making its shareable resources available to peers that request it. Pure and hybrid P2P instant messaging architectures are prohibited, since they bypass the security and auditing policies within the enclave.

Non-Computing Check: Request a copy of the policy prohibiting peer-to-peer applications or software. If no policy can be produced, then this is a finding.

Fix: Develop a policy that prohibits peer-to-peer applications.

Comments:							
Finding		Not a Finding		Not Reviewed		Not Applicable	

IM0020: Peer-to-peer applications are used for instant messaging

Vulnerability Key: V0015398

STIG ID: IM0020

Vulnerability: Peer-to-peer applications are used for instant messaging

IA Controls: ECSC-1 Security Configuration Compliance

Categories: 12.4 CM Process

Responsibility: Information Assurance Officer / System Administrator

References: Instant Messaging STIG

Severity: Category I

Vulnerability Discussion: Pure P2P networks operate with peers acting as equals and merge the roles of clients and server. Pure P2P has no central server managing the network. Hybrid P2P has a central server that keeps information on peers and responds to requests for that information. Peers are responsible for hosting available resources and for letting the central server know what resources they want to share, and for making its shareable resources available to peers that request it. Storing and hosting data on P2P networks increases the risk of information theft, unauthorized access, and data tampering. Pure and hybrid P2P instant messaging architectures are prohibited, since they bypass the security and auditing policies within the enclave.

.

Computing Check: Request the instant messaging application name or software being used for instant messaging. Check instant messaging application or software against the following list to ensure it is not peer-to-peer software. Not all P2P software can be listed here, so check the website and review the instant messaging documentation if necessary. If the software being used is listed here, then it is a finding.

- Caveat: This is not applicable if the P2P application has been authorized for use by the DAA. The IAO/SA must have approval documentation allowing the site to run the P2P application.

<u>Prohibited peer-to-peer software</u>

Kazza, Ares, BearShare, eMule, Morpheus, Limewire, BitTorrent, WinMx, EDonkey / Overnet, Shareaza, Buzm, CSpace, FastTrack, Freenet, GNUnet, Gnutella2, IRC, Kad Network, JXTA, Krawler, NeoEdge, P2PTV, PeerCasting, RetroShare, Tranche, Usenet, Windows Peer-to-Peer, WPNP, Vagaa, Zultrax, Shareaza, Napshare, MLDonkey, Kiwi Alpha, KCeasy, iMesh, Gnucleus, gift, FileScope, eMule, aMule.

Fix: Remove all peer-to-peer applications from the network immediately.

Comments:							
Finding		Not a Finding		Not Reviewed		Not Applicable	

IM0030: Publicly hosted instant messaging applications are being used for instant messaging

Vulnerability Key: V0015436

STIG ID: IM0030

Vulnerability: Publicly hosted instant messaging applications are being used for instant messaging.

IA Controls: ECSC-1 Security Configuration Compliance

Categories: 12.4 CM Process

Responsibility: Information Assurance Officer / System Administrator

References: Instant Messaging STIG

Severity: Category I

Vulnerability Discussion: Storing and hosting data on public servers increases the risk of information theft, unauthorized access, and data tampering. Hosting DoD information on public servers is prohibited due to the lack of security controls. DoD instant messaging systems should never store data on a public (.com) server or use a public (.com) switched network, since information could be exploited without the controls of an IAO. DoD instant messaging systems will use a client-to-server architecture and store all data on a private server (.mil) located behind a firewall.

Computing Check: Request the instant messaging application name or software being used for instant messaging. Check the instant messaging application or software against the following list to ensure it is not a publicly hosted instant messaging application. Not all publicly hosted instant messaging software can be listed here, so check the website and review the instant messaging documentation if necessary.

Prohibited publicly hosted instant messaging applications:

Adium, Agile Messenger, AIM (AOL Instant Messenger), aMSN, Ayttm, BitWise IM, BitBee, Centericq, climm, Coccinella, Cspace, Ebuddy, eMeSeNe, Exodus, Fire, Gajim, GCN, GOIM, Goofey, Google Talk, iChat, ICQ, IM2, imeem, IMVU, lnspeak, Instan-t, Interaction Chat, Jabbin, Kadu, Konnekt, Kopete, Licq, Mcabber, MECA Messenger, meebo, Meetro, Mercury

Messenger, MindSpring, Miranda IM, MySpaceIM, Naim, OcotoTalk, OpenWengo, Pandion, Paltalk, Pidgin, pork, Proteus, Psi, psyced, QIP, Qnext, QQ, RealtimeQuery, Skype, SIM, talk, Taotalk, Trillian, TrillianPro, Trillian Astra, Webex, Windows Live Messenger, Windows Messenger, Xfire, Yahoo Messenger, YSM, and Zephyr.

Caveat: Not applicable if instant messaging system is an outsourced Managed Enterprise Service for unclassified data in which the DAA has approved. Mark this check as Open Finding if the site does not have documentation from the DAA authorizing the use of an outsourced Managed Enterprise Service.

Fix: Remove all publicly hosted instant messaging software from the network.

Comments:							
Finding		Not a Finding		Not Reviewed		Not Applicable	

2.2 Instant Messaging Network Infrastructure

IM0040: Instant messaging servers are not located behind a firewall

Vulnerability Key: V0015401

STIG ID: IM0040

Vulnerability: Instant messaging servers are not located behind a firewall.

IA Controls: ECSC-1 Security Configuration Compliance

Categories: 4.3 Firewall

Responsibility: Information Assurance Officer / System Administrator

References: Instant Messaging STIG

Severity: Category I

Vulnerability Discussion: An enclave perimeter is the boundary between the private and locally managed side of a network and the public and usually provider-managed side of a network. A perimeter with access controls limiting only authorized traffic will prevent the potential attacks on servers. Instant messaging servers will be located behind a DoD enclave perimeter, providing access controls to prevent unauthorized access and tampering to server data. A firewall provides access controls allowing or disallowing public traffic from entering the enclave.

Computing Check: Check with the Network reviewer or system administrator to obtain the external, internal, and DMZ IP addresses of the firewall. Once these IP addresses have been obtained, review the IP address configuration on the instant messaging servers.

For windows servers, type the following at the command prompt:

```
c:>ipconfig /all
```

For UNIX server, type the following at the terminal:

```
#ifconfig –a
```

If the address is on the same internal network as the internal interface of the firewall, then this is not a finding. If the address is on the same network as the firewall DMZ interface, it may be a instant messaging gateway server. If is not a gateway server, then this is a finding. If the IP address is on the same network as the outside interface of the firewall, then this is a finding.

Fix: Locate all instant messaging servers behind a firewall.

Comments:							
Finding		Not a Finding		Not Reviewed		Not Applicable	

IM0050: Instant messaging clients connect to unapproved instant messaging servers

Vulnerability Key: V0015402

STIG ID: IM0050

Vulnerability: Instant messaging clients connect to unapproved instant messaging servers.

IA Controls: ECSC-1 Security Configuration Guide

Categories: 12.4 CM Process

Responsibility: Information Assurance Officer / System Administrator

References: Instant Messaging STIG

Severity: Category II

Vulnerability Discussion: Instant messaging clients may connect to any instant messaging server that will accept connections. If instant messaging clients are permitted to connect to unapproved instant messaging servers, the client machine may be infected with a viruses, Trojans, worms, adware, and spyware. Instant messaging clients will connect to only approved instant messaging servers.

Computing Check: Obtain the instant messaging servers IP addresses and hostnames from the systems administrator. Review the instant messaging client software configuration to verify that the client is configured to connect to these approved instant messaging servers. These servers will be listed as IP addresses or hostnames. If the clients are not configured to specified IP addresses or hostnames, then this is a finding.

Fix: Reconfigure instant messaging clients to connect to specified instant messaging servers.

Comments:							
Finding		Not a Finding		Not Reviewed		Not Applicable	

IM0060: Instant messaging gateway servers are not located in DMZ

Vulnerability Key: V0015403

STIG ID: IM0060

Vulnerability: Instant messaging gateway servers are not located in the DMZ.

IA Controls: ECSC-1 Security Configuration Compliance

Categories: 4.4 DMZ

Responsibility: Information Assurance Officer / System Administrator

References: Instant Messaging STIG

Severity: Category II

Vulnerability Discussion: A DMZ is a physical or logical subnetwork that usually contains an organization's external services to a larger, untrusted network, typically the Internet. The purpose of a DMZ is to add an additional layer of security to an organization's local area network (LAN). DoD Instruction 8500.2 requires a DMZ for confidentiality levels of High and Medium identified as classified and sensitive domains respectively. A DMZ provides boundary protection for instant messaging architectures that interconnect enclaves.

Computing Check: Obtain the network address of the DMZ from the network reviewer or system administrator. Check the IP address of the gateway instant messaging server to see if it is in the DMZ network range. If not, then this is a finding. If no gateway servers exist or are not required, then this check is Not Applicable.

For windows servers, type the following at the command prompt:

```
c:>ipconfig /all
```

For UNIX server, type the following at the terminal:

```
#ifconfig –a
```

Fix: Place the gateway server in the DMZ.

Comments:							
Finding		Not a Finding		Not Reviewed		Not Applicable	

IM0070: Instant messaging system communicates or interacts with public servers

Vulnerability Key: V0015404

STIG ID: IM0070

Vulnerability: Instant messaging system communicates or interacts with public servers.

IA Controls: ECSC-1 Security Configuration Compliance

Categories: 12.4 CM Process

Responsibility: Information Assurance Officer / System Administrator

References: Instant Messaging STIG

Severity: Category I

Vulnerability Discussion: Instant messaging servers can connect to any public instant messaging servers that will accept connections. If instant messaging servers are not configured to connect to specified servers, they may accept or connect to unapproved public servers. These connections may expose instant messaging servers to viruses, Trojans, worms, adware, and spyware, and potential attacks.

Computing Check: Review the instant messaging server configuration and examine the servers that it is configured to communicate with it. If any public IP addresses or hostnames are configured, then this is a finding.

Caveat: Not applicable if traversing an outsourced Managed Enterprise Service for unclassified data in which the DAA has approved.

Fix: Remove all public server configurations from the instant messaging system.

Comments:							
Finding		Not a Finding		Not Reviewed		Not Applicable	

IM0080: Instant messaging traffic is not encrypted

Vulnerability Key: V0015405

STIG ID: IM0080

Vulnerability: Instant messaging traffic is not encrypted

IA Controls: ECCT -1 Encryption for Confidentiality, ECCT-2 Encryption for Confidentiality

Categories: 8.1 Encryption for Data in Transit

Responsibility: Information Assurance Officer / System Administrator

References: Instant Messaging STIG

Severity: Category II

Vulnerability Discussion: Unencrypted traffic may be read, viewed, or modified by anyone that has access to the traffic. Plaintext traffic may be stored or logged on routers, switches, or servers while in transit. Unencrypted instant messaging sessions are also vulnerable to a number of attacks to include "man-in-the-middle" attacks, TCP Hijacking, and replay. All of these vulnerabilities result in a loss of privacy and data theft. Instant messaging systems will encrypt all traffic to ensure confidentiality.

Computing Check: Review the instant messaging topology diagrams to understand the architecture. Review the instant messaging server and client configurations to determine if encryption settings have been activated for all data in transit. Determine the encryption algorithms being used to ensure the algorithms are FIPS 140-2 compliant. See Appendix A. If instant messaging traffic is not encrypted with an approved FIPS 140-2 encryption algorithm, then this is a finding.

Fix: Encrypt all instant messaging traffic**.**

Comments:							
Finding		Not a Finding		Not Reviewed		Not Applicable	

IM0090: Instant messaging clients are not using DoD certificate authority

Vulnerability Key: V0015438

STIG ID: IM0090

Vulnerability: Instant messaging clients are not using DoD certificate authority.

IA Controls: DCNR-1 Non-repudiation, ECCT -1 Encryption for Confidentiality, ECCT-2 Encryption for Confidentiality
Categories: 1.2 PKI

Responsibility: Information Assurance Officer / System Administrator

References: Instant Messaging STIG

Severity: Category II

Vulnerability Discussion: Digital certificates bind each user's identity to his or her public key. Combined with the user's private key, this public key allows the user to be authenticated over open networks. Verifying that the PKI certificates are valid verify users and ensure that proper DoD certificates are being utilized. Secondly, encrypting sessions using FIPS 140-2 encryption algorithm requires a valid DoD certificate. Some clients may not verify the FIPS 140-2 encryption algorithm certificate received from the server. Without verifying the FIPS 140-2 encryption algorithm client certificate, data transported to and from the server is vulnerable to attackers. Unencrypted instant messaging traffic may be from being read or viewed by anyone, and this traffic may contain sensitive information. Unencrypted instant messaging sessions are vulnerable to a number of attacks to include "man-in-the-middle" attacks, TCP Hijacking, and replay.

Computing Check: Review the instant message client application to see if encryption is enabled. Then review the certificates listed on the instant messaging client. These certificates are used to validate a server's PKI certificate when initiating a SSL/TLS or IPSEC connection. Validate the certificate is listed in the InstallRoot3.0_SAG.pdf document. The DoD certificates that are listed in the InstallRoot3.0_SAG.pdf document are listed in Appendix B. If the certificate is not listed here, then this is a finding.

NOTE: The InstallRoot3.0.1_SAG.pdf document can be downloaded from the following link: https://gesportal.dod.mil/sites/dodpke/download.aspx. Select the InstallRoot v3.0.1 Download and unzip it to get the document.

Fix: Configure instant messaging clients to use DoD certificate authority.

Comments:							
Finding		Not a Finding		Not Reviewed		Not Applicable	

IM0100: Instant messaging services not required are enabled.

Vulnerability Key: V0015439

STIG ID: IM0100

Vulnerability: Instant messaging services not required are enabled. Required services will be documented with the IAO/SA.

IA Controls: ECSC-1 Security Configuration Compliance

Categories: 12.4 CM Process

Responsibility: Information Assurance Officer / System Administrator

References: Instant Messaging STIG

Severity: Category II

Vulnerability Discussion: Instant messaging servers provide communication to users such as user registration, authentication, instant messaging, account management, logging, and software downloads. Some services are necessary for the functionality and availability of the instant messaging server. Services not required for operation will be disabled to prevent potential vulnerabilities and attacks on these services.

Computing Check: Request a copy of the required services documentation from the IAO/SA for the instant messaging system. Compare this list of required services to the actual running services on the instant messaging system. For Windows servers, go to the control panel, administrative tools, and services to view active services. For UNIX servers, go to the terminal and type the following:
#ps –ef

Any services that are not documented found running would be a finding.

Fix: Document all required services and disable those not required.

Comments:							
Finding		Not a Finding		Not Reviewed		Not Applicable	

IM0110: There is no topology diagram of the instant messaging system

Vulnerability Key: V0015440

STIG ID: IM0110

Vulnerability: There is no topology diagram of the instant messaging system.

IA Controls: ECSC-1 Security Configuration Compliance, DCID-1 Interconnection Documentation

Categories: 12.9 Documentation

Responsibility: Information Assurance Officer / System Administrator

References: Instant Messaging STIG

Severity: Category III

Vulnerability Discussion: An instant messaging infrastructure design will be documented and represented using topology diagrams. Representing the instant messaging infrastructure through topology diagrams shows the overall layout of the infrastructure and where servers and data are physically located. Creating topology diagrams provide a graphical representation of the security architecture, inter-connectivity between servers, and the functionality of the instant messaging infrastructure. The topology diagram will illustrate the network and enclave boundaries, server locations within enclaves, server-to-server communications, client-to-server communications, databases, and directory services. The diagram will also reference ports used by all server-to-server communications and client-to-server communications.

Non-Computing Check: Request a copy of the instant messaging topology diagram. Review the diagram to validate the following:

- Network boundaries
- Servers
- Databases
- Client access points
- IP Subnets
- Ports used for instant messaging traffic.

If the topology diagram does not exist or is incomplete, then this is a finding.

Fix: Develop and maintain an accurate instant messaging topology diagram.

Comments:							
Finding		Not a Finding		Not Reviewed		Not Applicable	

2.3 Instant Messaging Authentication

IM0130: Instant messaging username policy does not exist

Vulnerability Key: V0015441

STIG ID: IM0130

Vulnerability: Instant messaging username policy does not exist.

IA Controls: ECSC-1 Security Configuration Compliance

Categories: 12.4 CM Process

Responsibility: Information Assurance Officer / System Administrator

References: Instant Messaging STIG

Severity: Category III

Vulnerability Discussion: Instant messaging usernames should be acceptable and appropriate for the work environment. Instant messaging usernames that are confusing, misleading, disruptive, or offensive are inappropriate for use within the DoD. If usernames are created in this manner, tracking actual identities of users becomes difficult.

Non-Computing Check: Request a copy of the instant messaging usernames policy to review it. If no policy can be produced, then this is a finding.

Fix: Create an instant messaging usernames policy that defines the proper creation of usernames.

Comments:							
Finding		Not a Finding		Not Reviewed		Not Applicable	

IM0140: Instant messaging usernames are not in accordance with the username policy

Vulnerability Key: V0015442

STIG ID: IM0140

Vulnerability: Instant messaging usernames are not in accordance with the username policy.

IA Controls: ECSC-1 Security Configuration Compliance

Categories: 12.4 CM Process

Responsibility: Information Assurance Officer / System Administrator

References: Instant Messaging STIG

Severity: Category III

Vulnerability Discussion: Instant messaging usernames should be acceptable and appropriate for the work environment. Instant messaging usernames that are confusing, misleading, disruptive, or offensive are inappropriate for instant messaging systems. If usernames are created in this manner, tracking actual identities of users becomes difficult.

Computing Check: Review the instant messaging usernames on the instant messaging system to see if they meet the instant messaging username policy. If usernames do not match the username policy, then this is a finding.

Fix: Create instant messaging usernames according the usernames policy.

Comments:							
Finding		Not a Finding		Not Reviewed		Not Applicable	

IM0150: Instant messaging system is not linked to a directory service

Vulnerability Key: V0015443

STIG ID: IM0150

Vulnerability: Instant messaging system is not linked to a directory service.

IA Controls: ECSC-1 Security Configuration Compliance, IAAC-1 Account Control

Categories: 1.3 Identity Management

Responsibility: Information Assurance Officer / System Administrator

References: Instant Messaging STIG

Severity: Category II

Vulnerability Discussion: Directory services are commonly responsible for managing and providing access to critical organization data. This is true of directory services in which identification, authentication, and authorization data is stored for reference by operating systems or applications. Users are identified, authenticated, and authorized by the directory service before being granted access to the instant messaging system. Storing instant messaging system user information on the local instant messaging system may not provide the necessary security for this information.

Computing Check: Review the configuration of the instant messaging system to examine the settings that link the instant messaging system with the directory services. To verify the link is functioning, review the logs to see if synchronization is occurring. If the instant messaging system is not linked to a directory service, then this is a finding.

Fix: Configure the instant messaging system to link its users to a directory service.

Comments:							
Finding		Not a Finding		Not Reviewed		Not Applicable	

IM0160: There are no documented procedures for adding or deleting users

Vulnerability Key: V0015444

STIG ID: IM0160

Vulnerability: There are no documented procedures for adding and deleting instant messaging users.

IA Conrols: IAAC-1 Account Controls

Categories: 12.4 CM Process

Responsibility: Information Assurance Officer / System Administrator

References: Instant Messaging STIG

Severity: Category III

Vulnerability Discussion: Instant messaging users that are no longer active and not removed from the system could pose a security risk to the community. If the username was compromised, then it could appear to other uses as a valid user even though the user was supposed to be removed. Usernames that are added incorrectly may not have the correct permissions or privileges. Therefore, there will be documented procedures for adding and deleting instant messaging users to ensure users are added and removed correctly. Furthermore, as personnel changes occur, this ensures new employees will follow the correct procedure.

Non-Computing Check: Request a copy of the username procedures for creating and deleting users for the instant messaging system. If no documented procedures can be produced, then this is a finding.

Fix: Develop user creation and deletion procedures for the instant messaging system.

Comments:

Finding		Not a Finding		Not Reviewed		Not Applicable	

IM0170: User passwords are not in accordance with policy

Vulnerability Key: V0015445

STIG ID: IM0170

Vulnerability: User passwords are not in accordance with DoD password policy.

IA Controls: IAIA-1 Individual Identification and Authentication, IAIA-2 Individual Identification and Authentication

Categories: 1.1 Passwords

Responsibility: Information Assurance Officer / System Administrator

References: Instant Messaging STIG

Severity: Category II

Vulnerability Discussion: Passwords not created according to the DoDI 8500.2 policy, are considered easy to guess and crack. Passwords that are easy to guess refers to passwords created using a word, phrase or number that has special meaning to the user, such as a name, their birthday, or social security number. An intruder who knows something about the user may be able to guess the password. Passwords that are easy to crack refers to passwords that are created using words from the dictionary. Using words from the dictionary creates vulnerabilities because "brute force" methods and "dictionary" attacks can crack them.

Computing Check: Review the password setting policy on the instant messaging system. If it is linked to a directory service, then review these settings. Ensure they meet the following characteristics:

- A minimum of 9 characters
- Include at least one uppercase alphabetic character
- Include at least one lowercase alphabetic character
- Include at least one number
- Include at least one non-alphanumeric (special) character
- Expire after 60 days

Example: DemPa3*2!
If they do not meet these characteristics, then this is a finding.

Note: Password length may vary depending on the INFOCON notice.

Fix: Configure passwords to be 9 characters in length with a character mix of upper case letters, lower case letters, numbers, and special characters, including at least one of each.

Comments:							
Finding		Not a Finding		Not Reviewed		Not Applicable	

IM0180: System administrator passwords are not in accordance with policy

Vulnerability Key: V0015446

STIG ID: IM0180

Vulnerability: System administrator passwords are not in accordance with DoD password policy.

IA Controls: IAIA-1 Individual Identification and Authentication, IAIA-2 Individual Identification and Authentication

Categories: 1.1 Passwords

Responsibility: Information Assurance Officer / System Administrator

References: Instant Messaging STIG

Severity: Category II

Vulnerability Discussion: Passwords not created according to the DoDI 8500.2 policy, are considered easy to guess and crack. Passwords that are easy to guess refers to passwords created using a word, phrase or number that has special meaning to the user, such as a name, their birthday, or social security number. An intruder who knows something about the user may be able to guess the password. Passwords that are easy to crack refers to passwords that are created using words from the dictionary. Using words from the dictionary creates vulnerabilities because “brute force” methods and “dictionary” attacks can crack them.

Computing Check: Review the password setting policy on the instant messaging system. System administrator passwords will be 14 characters in length with the following characteristics:
- A minimum of 14 characters
- Include at least one uppercase alphabetic character

- Include at least one lowercase alphabetic character
- Include at least one number
- Include at least one non-alphanumeric (special) character
- Expire after 60 days

Example: DemPa3*2!IS23@a
If they do not meet these characteristics, then this is a finding.

Note: Password length may vary depending on the INFOCON notice.

Fix: Configure passwords to be 14 characters in length with a character mix of upper case letters, lower case letters, numbers, and special characters, including at least one of each.

Comments:							
Finding		Not a Finding		Not Reviewed		Not Applicable	

IM0190: Instant messaging system stored passwords are not encrypted

Vulnerability Key: V0015406

STIG ID: IM0190

Vulnerability: Instant messaging system stored passwords are not encrypted.

IA Controls: IAIA-1 Individual Identification and Authentication, IAIA-2 Individual Identification and Authentication

Categories: 1.1: Passwords, 8.2 Encrypting Data at Rest

Responsibility: Information Assurance Officer / System Administrator

References: Instant Messaging STIG

Severity: Category II

Vulnerability Discussion: Protecting stored passwords is important since there are so many avenues to attack a system. Attacks may be launched against the operating system, the database server application, the custom application interface, the client interface, etc. Any attack providing system-level access to an attacker is a risk to data at rest, including passwords. Systems are also potential targets for a multitude of computer viruses, worms, and Trojans. Passwords that are unencrypted may be viewed, copied, or modified by anyone who has access to the system.

Computing Check: Review the instant messaging system password file. If the instant messaging system is linked to a directory service, then view this file. If the passwords are readable, then this is a finding.

Fix: Encrypt all passwords stored on the instant messaging system.

Comments:							
Finding		Not a Finding		Not Reviewed		Not Applicable	

IM0200: Anonymous and guest users are enabled

Vulnerability Key: V0015447

STIG ID: IM0200

Vulnerability: Anonymous and guest users are enabled.

IA Controls: IAIA-1 Individual Identification and Authentication, IAIA-2 Individual Identification and Authentication

Categories: 1.3 Identity Management

Responsibility: Information Assurance Officer / System Administrator

References: Instant Messaging STIG

Severity: Category II

Vulnerability Discussion: Only authorized users should be utilizing the instant messaging system through the use of valid user accounts. Anonymous and guest user accounts are usually used for users that do not have valid instant messaging system user accounts. These usernames may be used by unauthorized users to gain access to the system and view information that may assist them to gain elevated privileges to the system. Disabling these accounts mitigates this vulnerability.

Computing Check: Review the instant messaging system configuration to verify that anonymous and guest user accounts are disabled. If these accounts are not disabled, then this is a finding.

Fix: Disable the anonymous and guest user accounts.

Comments:							
Finding		Not a Finding		Not Reviewed		Not Applicable	

IM0210: Unsuccessful logon attempts is not configured to three with account lockout of 15 minutes

Vulnerability Key: V0015448

STIG ID: IM0210

Vulnerability: Unsuccessful logon attempts is not configured to three with an account lockout of 15 minutes or until it is unlocked.

IA Controls: IAAC-1 Control Board

Categories: 1.4 Authentication Services Identity Management

Responsibility: Information Assurance Officer / System Administrator

References: Instant Messaging STIG

Severity: Category II

Vulnerability Discussion: Given enough time and potential to try multiple username and password combinations an attacker might eventually succeed in compromising the security of a server or other computer. Account lockout policies configure thresholds to automatically shut down an account if too many incorrect username and password combinations are attempted in order to protect the machine.

Computing Check: Review the instant messaging system configuration to verify the account lockout policy is set to 3 unsuccessful logins, and the lockout period is 15 minutes at a minimum. If these two settings are not configured, then this is a finding.

Fix: Configure the account lockout to 3 unsuccessful logins, and lockout period to 15 minutes at the minimum.

Comments:							
Finding		Not a Finding		Not Reviewed		Not Applicable	

2.4 Instant Messaging Logging

Instant messaging systems will differ on their logging configuration and settings. Some systems may use distinct logging for user events, system events, virtual meetings, meeting tools, etc., while others may group them together. Work with the system administrator to locate these logs, verify their location, and determine if the check applies to the instant messaging system.

IM0220: Instant messaging system does not log user events

Vulnerability Key: V0015449

STIG ID: IM0220

Vulnerability: Instant messaging system does not log user events.

IA Controls: ECAT-1 Audit, Trail, Monitoring, Analysis, and Reporting, ECAT-2 Audit, Trail, Monitoring, Analysis, and Reporting

Categories: 10.4 Reporting

Responsibility: Information Assurance Officer / System Administrator

References: Instant Messaging STIG

Severity: Category II

Vulnerability Discussion: Systems that do log user events will not have the ability to review past system and user events. Recording these events is critical to establishing a recorded history of system events, enabling system administrators to diagnose intermittent system problems, suspicious user activity, and assisting with investigations. Log events also verify that the established policies configured on the system are in fact working as configured.

Computing Check: Review the instant messaging system configuration and log files to verify user logins and resource access are recorded. User events include the following:

- Successful logins and failed logins
- Successful resource access and failed resource access.

If these are not logged, then this is a finding.

Fix: Configure the instant messaging system to log user events.

Comments:

Finding		Not a Finding		Not Reviewed		Not Applicable	

IM0230: Instant messaging system does not log system events

Vulnerability Key: V0015450

STIG ID: IM0230

Vulnerability: Instant messaging system does not log system events.

IA Controls: ECAT-1 Audit, Trail, Monitoring, Analysis, and Reporting, ECAT-2 Audit, Trail, Monitoring, Analysis, and Reporting

Categories: 10.4 Reporting

Responsibility: Information Assurance Officer / System Administrator

References: Instant Messaging STIG

Severity: Category II

Vulnerability Discussion: Systems that do log system events will not have the ability to review past system and user events. Recording system events is critical to establishing a recorded history of system events, enabling system administrators to diagnose intermittent system problems, suspicious user activity, and assisting with investigations. Log events also verify that the established policies configured on the system are in fact working as configured.

Computing Check: Review the instant messaging system configuration and log files to verify user system events are being recorded. System events include the following:

- Instant messaging system configuration changes
- Instant messaging daemon or service stop and starts
- Instant messaging system warning and error messages

If these are not logged, then this is a finding.

Fix: Configure the instant messaging system to log system events.

Comments:

Finding		Not a Finding		Not Reviewed		Not Applicable	

IM0240: Instant messaging system does not log virtual meeting entries and exits

Vulnerability Key: V0015451

STIG ID: IM0240

Vulnerability: Instant messaging system does not log virtual meeting entries and exits.

IA Controls: ECAR-1 Audit Record Content, ECAR-2 Audit Record Content

Categories: 10.4 Reporting

Responsibility: Information Assurance Officer / System Administrator

References: Instant Messaging STIG

Severity: Category II

Vulnerability Discussion: Systems that do log virtual meeting entries and exits will not have the ability to review past virtual meeting attendances. Recording these events is critical to establishing a recorded history of all virtual meetings and who attended and left the meetings. Logging these events will also verify that virtual meetings are attended by authorized persons only.

Computing Check: Review the instant messaging system configuration and log files to verify virtual meetings entries and exits are logged. If these events are not logged, then this is a finding.

Fix: Configure the instant messaging system to record virtual meeting entries and exits.

Comments:							
Finding		Not a Finding		Not Reviewed		Not Applicable	

IM0250: Instant messaging system does not log virtual meeting tools

Vulnerability Key: V0015452

STIG ID: IM0250

Vulnerability: Instant messaging system does not log virtual meeting tools.

IA Controls: ECAR-1 Audit Record Content, ECAR-2 Audit Record Content

Categories: 10.4 Reporting

Responsibility: Information Assurance Officer / System Administrator

References: Instant Messaging STIG

Severity: Category II

Vulnerability Discussion: Systems that do log virtual meeting tools used during virtual meetings will not have the ability to review what tools were used during meetings. Recording these events is critical to establishing a recorded history of all virtual meetings and what tools were used. Logging these events will also verify that virtual meeting tools are restricted to authorized users only.

Computing Check: Review the instant messaging system configuration to verify that virtual meeting tools used during meetings are logged. If the tools used are not logged, then this is a finding.

Fix: Configure all virtual meetings to log all meeting tools used.

Comments:							
Finding		Not a Finding		Not Reviewed		Not Applicable	

IM0310: Instant messaging system logs are not stored offline for a year

Vulnerability Key: V0015453

STIG ID: IM0310

Vulnerability: Instant messaging system logs are not stored offline for a year.

IA Controls: ECRR-1 Audit Record Retention

Categories: 10.4 Reporting, 10.5 Retention

Responsibility: Information Assurance Officer / System Administrator

References: Instant Messaging STIG

Severity: Category II

Vulnerability Discussion: Storing log files offline provides a way to recover these files in case an investigation is necessary. Typically these files are stored offline on tape media or external networks. Log files enable the enforcement of individual accountability by creating a reconstruction of events. They also assist in problem identification that may lead to problem resolution. If these log files are not retained, there is no way to trace or reconstruct the events, and if it was discovered the network was hacked, there would be no way to trace the full extent of the compromise.

Computing Check: Review the instant messaging system offline log files. If they are offsite, review the process to move them to this alternative site. Verify that the log files are retained for at least one year at a minimum. If the log files are not stored offline for a minimum of one year, then this is a finding.

Fix: Configure the instant messaging system to store log files offline for a minimum of one year.

Comments:							
Finding		Not a Finding		Not Reviewed		Not Applicable	

IM0320: No centralized syslog server is deployed

Vulnerability Key: V0015454

STIG ID: IM0320

Vulnerability: No centralized syslog server is deployed for the instant messaging system.

IA Controls: ECRR-1 Audit Record Retention

Categories: 10.4 Reporting, 10.5 Retention

Responsibility: Information Assurance Officer / System Administrator

References: Instant Messaging STIG

Severity: Category III

Vulnerability Discussion: Syslog addresses the problem of information overload by breaking down log data into categories that can be easily managed and analyzed. Without a centralized syslog, detection of attacks is limited, and each individual system will need to be configured and reviewed separately. A centralized syslog server provides visibility into the network activity, a central repository for host logs, one location for backing up or analyzing log files, and the correlation of data across many diverse systems. A syslog server can make sure devices are working properly. For example, if a instant messaging system is supposed to be blocking a certain type of traffic that appears in a syslog entry, it means something is not working or is configured incorrectly.

Computing Check: Locate the centralized syslog server and verify the instant messaging system is sending its logs to the server. If no centralized syslog server exists or the instant messaging system is not sending its logs there, then this is a finding.

Fix: Configure the instant messaging system to send its log files to the syslog server.

Comments:							
Finding		Not a Finding		Not Reviewed		Not Applicable	

IM0330: Instant messaging system logs are not restricted to authorized users only

Vulnerability Key: V0015455

STIG ID: IM0330

Vulnerability: Instant messaging system logs are not restricted to authorized users only. These authorized users will be documented.

IA Controls: ECCD-1 Changes to Data, ECCD-2 Changes to Data

Categories: 2.1 Object permissions

Responsibility: Information Assurance Officer / System Administrator

References: Instant Messaging STIG

Severity: Category II

Vulnerability Discussion: Only authorized users will be configured to review and modify instant messaging system logs. If these logs are not configured with access controls, unauthorized users may view, read, copy, modify, or delete these logs. These logs provide the enforcement of individual accountability by creating a reconstruction of events. They also assist in problem identification that may lead to problem resolution. If these log files are modified, there is no way to trace or reconstruct the events, and if it was discovered the network hacked, there would be no way to trace the full extent of the break in.

Computing Check: Review the instant messaging system access controls to the log files. Verify that only authorized users are listed. These authorized users will be documented, so compare the configured users to the documented users to ensure they match. If there are no documented users, or no restrictions to the log files, then this is a finding.

Fix: Configure the instant messaging system with access controls restricting log file access to authorized users only.

Comments:							
Finding		Not a Finding		Not Reviewed		Not Applicable	

IM0340: Instant messaging system logs are not reviewed

Vulnerability Key: V0015735

STIG ID: IM0340

Vulnerability: Instant messaging system logs are not reviewed.

IA Controls: ECAT-1 Audit, Trail, Monitoring, Analysis, and Reporting, ECAT-2 Audit, Trail, Monitoring, Analysis, and Reporting

Categories: 10.4 Reporting

Responsibility: Information Assurance Officer / System Administrator

References: Instant Messaging STIG

Severity: Category II

Vulnerability Discussion: It is necessary to review instant messaging system logs, or suspicious activity, problems, attacks, or system warnings will go undetected. These logs provide visibility into the activities and events of the instant messaging system. These logs enable system administrators and auditors the ability to recreate past events, monitor the system, and ensure security policies are being enforced.

Non-Computing Check: Ask the IAO/SA how often they review the instant messaging system logs. Ideally, they should be reviewed daily. If the logs are not reviewed, or rarely, then this is a finding.

Fix: The IAO/SA will review all instant messaging system logs regularly.

Comments:							
Finding		Not a Finding		Not Reviewed		Not Applicable	

2.5 Instant Messaging System Configuration

IM0350: No warning banner configured on instant messaging system

Vulnerability Key: V0015457

STIG ID: IM0350

Vulnerability: No warning banner configured on instant messaging system.

IA Controls: ECWM-1 Warning Message

Categories: 11.6 Warning Banners

Responsibility: Information Assurance Officer / System Administrator

References: Instant Messaging STIG

Severity: Category II

Vulnerability Discussion: To successfully prosecute unauthorized users who improperly use a instant messaging system, a warning banner must be displayed. The warning banner must warn authorized and unauthorized users about what is considered the proper use of the instant messaging system, that the system is being monitored to detect improper use and other illicit activity, that there is no expectation of privacy while using the instant messaging system.

Computing Check: Review the instant messaging system configuration and login to the system to verify a warning banner is displayed. If no warning banner is displayed or it does not have all the requirements, then this is a finding.
Warning Banner must contain the following:

```
You are accessing a U.S. Government (USG) Information System (IS) that is
provided for USG-authorized use only.

By using this IS (which includes any device attached to this IS), you
consent to the following conditions:

-The USG routinely intercepts and monitors communications on this IS for
purposes including, but not limited to, penetration testing, COMSEC,
monitoring, network operations and defense, personnel misconduct (PM), law
enforcement (LE), and counterintelligence (CI) investigations.
```

-At any time, the USG may inspect and seize data stored on this IS.

-Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.

-This IS includes security measures (e.g., authentication and access controls) to protect USG interests-not for your personal benefit or privacy.

-Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.

Fix: Implement a warning banner on the instant messaging system that is presented to all users.

Comments:							
Finding		Not a Finding		Not Reviewed		Not Applicable	

IM0360: Instant messaging servers are not OS STIG compliant

Vulnerability Key: V0015458

STIG ID: IM0360

Vulnerability: Instant messaging servers are not configured according to the operating system STIG.

IA Controls: ECSC-1 Security Configuration Compliance

Categories: 12.4 CM Process

Responsibility: Information Assurance Officer / System Administrator

References: Instant Messaging STIG

Severity: Category II

Vulnerability Discussion: There are a significant number of vulnerabilities with UNIX and Windows operating systems. The DoD publishes operating systems STIGs to mitigate these vulnerabilities and provide a baseline configuration for all operating systems before connecting these systems to the DISN. Not configuring instant messaging systems with the appropriate operating STIG will leave numerous vulnerabilities open that may be exploited by attacks.

Computing Check: Work with the OS reviewer to determine if the instant messaging servers have been configured according to the appropriate OS STIG. If not, then this is a finding.

Fix: Configure all instant messaging system with the appropriate OS STIG.

Comments:							
Finding		Not a Finding		Not Reviewed		Not Applicable	

IM0370: Instant messaging system databases are not STIG compliant

Vulnerability Key: V0015459

STIG ID: IM0370

Vulnerability: Instant messaging system databases are not configured according to the Database STIG.

IA Controls: ECSC-1 Security Configuration Compliance

Categories: 12.4 CM Process

Responsibility: Information Assurance Officer / System Administrator

References: Instant Messaging STIG

Severity: Category II

Vulnerability Discussion: There are a significant number of vulnerabilities with databases. The DoD publishes the Database STIG and checklists to mitigate these vulnerabilities and provide a baseline configuration for all databases before connecting these systems to the DISN. Not configuring instant messaging systems with the Database STIG and checklist will leave numerous vulnerabilities open that may be exploited by attacks.

Computing Check: Work with the database reviewer to determine if the instant messaging system databases have been configured according to the Database STIG. If not, then this is a finding.

Fix: Configure the instant messaging system with the Database STIG and checklists.

Comments:							
Finding		Not a Finding		Not Reviewed		Not Applicable	

IM0380: The IAO/SA does not subscribe to instant messaging system patches or update notices

Vulnerability Key: V0015396

STIG ID: IM0380

Vulnerability: The IAO/SA does not subscribe to instant messaging system patches or update notices.

IA Controls: ECSC-1 Security Configuration Compliance

Categories: 12.4 CM Process

Responsibility: Information Assurance Officer / System Administrator

References: Instant Messaging STIG

Severity: Category III

Vulnerability Discussion: If the IAO/SA does not subscribe to vendor security, patch, or update notices, the IAO/SA will not be informed of potential vulnerabilities in the instant messaging system. These potential vulnerabilities may be exploited on the instant messaging system, and the IAO/SA would not be aware that specific patches are available to close these vulnerabilities. Subscribing to vendor security, patch, and upgrade notices ensures that the latest vulnerabilities are known and evaluated against the instant messaging system.

Non-Computing Check: Request the IAO/SA produce past security, patch, or update notifications that were received due to their subscription to these notices. If these cannot be produced, then this is a finding.

Fix: Subscribe to instant messaging system vendor notifications.

Comments:							
Finding		Not a Finding		Not Reviewed		Not Applicable	

IM0390: Instant messaging servers and clients are not patched

Vulnerability Key: V0015461

STIG ID: IM0390

Vulnerability: Instant messaging servers and clients are not configured with the latest patches and updates.

IA Controls: ECSC-1 Security Configuration Compliance

Categories: 12.4 CM Process

Responsibility: Information Assurance Officer / System Administrator

References: Instant Messaging STIG

Severity: Category II

Vulnerability Discussion: Software patches and updates are software designed to update or fix problems with a computer program or its supporting data. This includes fixing bugs, replacing graphics and improving the usability or performance. Instant messaging servers and clients that do not have the latest patches or updates installed have potential vulnerabilities that may be exploited.

Computing Check: Review the instant messaging server and client versions and compare these to the vendors latest released patches. If these are not the same, then this is a finding.

Fix: Apply the latest updates and patches to the instant messaging system.

Comments:							
Finding		Not a Finding		Not Reviewed		Not Applicable	

IM0400: Remote administration to instant messaging servers is not restricted to authorized IP addresses

Vulnerability Key: V0015462

STIG ID: IM0400

Vulnerability: Remote administration to instant messaging servers is not restricted to authorized IP addresses.

IA Controls: ECSC-1 Security Configuration Compliance

Categories: 2.2 Least Privilege

Responsibility: Information Assurance Officer / System Administrator

References: Instant Messaging STIG

Severity: Category II

Vulnerability Discussion: When remote management of a instant messaging server is required, access lists or filters must be used to limit which hosts may connect to the server using management applications. Without these filters, anyone on the network may connect to the server to gather information about the instant messaging server configuration, potential vulnerabilities, or launch attacks. Restricting remote administration to instant messaging servers by specific IP addresses decreases the likelihood of these activities.

Computing Check: Work with the network reviewer or system administrator to review the instant messaging server or router configurations to verify that only approved IP addresses may remotely connect for remote administration. These authorized IP addresses will be documented with the IAO/SA. Verify that the documented and configured IP addresses match. If these are not configured or they are not documented, then this is a finding.

Fix: Configure and document the approved IP addresses for remote management of the instant messaging servers.

Comments:							
Finding		Not a Finding		Not Reviewed		Not Applicable	

IM0410: Remote administration traffic is not encrypted

Vulnerability Key: V0015463

STIG ID: IM0410

Vulnerability: Remote administration traffic is not encrypted.

IA Controls: ECCT-1 Encryption for Confidentiality, ECCT-2 Encryption for Confidentiality

Categories: 8.1 Encrypted Data in Transit

Responsibility: Information Assurance Officer / System Administrator

References: Instant Messaging STIG

Severity: Category II

Vulnerability Discussion: Unencrypted traffic may be read, viewed, or modified by anyone that has access to the traffic. Plaintext traffic may be stored or logged on routers, switches, or servers while in transit. Unencrypted administration sessions are also vulnerable to a number of attacks to include “man-in-the-middle” attacks, TCP Hijacking, and replay. All of these vulnerabilities result in a loss of privacy and data theft. Instant messaging systems will encrypt all traffic to ensure confidentiality.

Computing Check: Review the client and server configurations to ensure that remote administration is configured with a FIPS 140-2 encryption algorithm. If the remote administration traffic is not encrypted with a FIPS 140-2 encryption algorithm, then this is a finding.

Fix: Encrypt remote administration traffic.

Comments:							
Finding		Not a Finding		Not Reviewed		Not Applicable	

IM0420: Instant messaging servers do not have antivirus or Host Based IDS

Vulnerability Key: V0015464

STIG ID: IM0420

Vulnerability: Instant messaging servers do not have antivirus or Host Based IDS.

IA Controls: ECVP-1 Virus Protection, ECID-1 Host Based IDS

Categories: 14.7 Antivirus, 14.6 HIDS/Personal Firewalls

Responsibility: Information Assurance Officer / System Administrator

References: Instant Messaging STIG

Severity: Category II

Vulnerability Discussion: Malicious software (Malware) is any program or file that is harmful to a computer. Malware includes computer viruses, worms, Trojan horses, and spyware. Malware has the capability to corrupt files, alter or delete data, distribute confidential data, disable hardware, deny legitimate user access, and cause hard drives to crash. Antivirus software removes and detects viruses and other spyware. Host based IDS is used to detect several types of malicious behaviors that can compromise the security and trust of a computer system. These behaviors include network attacks against vulnerable services, data driven attacks on applications, host based attacks such as privilege escalation, unauthorized logins and access to sensitive files, and malware (viruses, Trojan horses, and worms).Without antivirus support and host based IDS, servers are vulnerable to malware and other attack vectors.

Computing Check: Review the instant messaging server configuration to ensure that antivirus and host based IDS are installed. The approved JTF-GNO antivirus software vendors are Mcafee, Symantec, and Trend Micro. The approved HIDS software is HBSS. If antivirus or HIDS packages are not installed on the server, then this is a finding.

Fix: Install antivirus and host based IDS software on all instant messaging servers.

Comments:							
Finding		Not a Finding		Not Reviewed		Not Applicable	

IM0430: Instant messaging servers are not located in controlled access area

Vulnerability Key: V0015407

STIG ID: IM0430

Vulnerability: Instant messaging servers are not located in a controlled access area.

IA Controls: PEPF-1 Physical Protection of Facilities, PEPF-2 Physical Protection of Facilities

Categories: 5.11 Controlled Access Area (CAA)

Responsibility: Information Assurance Officer / System Administrator

References: Instant Messaging STIG

Severity: Category II

Vulnerability Discussion: Instant messaging servers may contain an aggregate of sensitive and non-sensitive data. Data that may be on the servers include instant messaging text, meeting tools content, log files, usernames, passwords, etc. If this data is not located in a controlled access area, unauthorized users may gain access to the server and have access to the data. This access may result in the loss of privacy and data theft.

Computing Check: Review the location of the instant messaging servers. Ensure that authorized users are required to verify their identity and authority before gaining access to the instant messaging servers. If the servers are not located in a controlled access area, then this is a finding.

Fix: Place all instant messaging servers in a controlled access area.

Comments:							
Finding		Not a Finding		Not Reviewed		Not Applicable	

2.6 Ports and Protocols Registration System

IM0440: Instant messaging system is not configured in accordance with PPS

Vulnerability Key: V0015408

STIG ID: IM0440

Vulnerability: Instant messaging system is not configured in accordance with the PPS CAL. The ports, protocols, and services for the instant messaging system are not documented with the IAO/SA.

IA Controls: DCPP-1 Ports, Protocols, and Services

Categories: 12.4 CM Process

Responsibility: Information Assurance Officer / System Administrator

References: Instant Messaging STIG

Severity: Category II

Vulnerability Discussion: The Ports, Protocols, and Services Category Assignment Lists maintains a list of ports, protocols, and services that have been evaluated for use on the DoD network. This list contains low, medium, and high assurance ports, protocols, and services. How these ports are configured is critical to protecting the LAN from attack. Standard port assignments and access methods have been set up to maximize security features and policy implementation. Instant messaging systems must meet these requirements.

Computing Check: Request the documentation with the list of all the open ports, protocols, and services for the instant messaging system from the IAO/SA. Work with the network reviewer or system administrator to review the ports and protocols used to communicate with all external servers and clients. Validate all ports, protocols, and services communicating with external servers and clients meet the PPS CAL assurance requirements. The PPS CAL is located at the http://iase.disa.mil. Ports may utilize Network Address Translation (NAT) at the firewall and/or router enclave over PPS approved ports, which meets the requirement. If the ports and protocols used by the instant messaging system do not meet the PPS CAL, then this is a finding.

Fix: Configure the instant messaging system or network to use only approved ports and protocols.

Comments:							
Finding		Not a Finding		Not Reviewed		Not Applicable	

IM0450: The Instant messaging system is not registered in the Ports and Protocols Registration System

Vulnerability Key: V0015465

STIG ID: IM0450

Vulnerability: The instant messaging system is not registered in the Ports and Protocols Registration system.

IA Controls: DCPP-1 Ports, Protocols, and Services

Categories: 12.4 CM Process

Responsibility: Information Assurance Officer / System Administrator

References: Instant Messaging STIG

Severity: Category III

Vulnerability Discussion: The Ports, Protocols, and Services Category Assignment Lists maintains a list of ports, protocols, and services that have been evaluated for use on the DoD network. This list contains low, medium, and high assurance ports, protocols, and services. How these ports are configured is critical to protecting the LAN from attack. Standard port assignments and access methods have been set up to maximize security features and policy implementation. Instant messaging systems will be registered as automated information systems (AIS) with their associated TCP or UDP ports in the DoD Ports and Protocol Registration System.

Non-Computing Check: Ask the IAO/SA if all instant messaging system ports and protocols are registered in the DoD Ports and Protocols registration system. If access is available, review the pnp.cert.smil.mil website to ensure all instant messaging ports and protocols are registered. If the instant messaging ports and protocols are not registered, then this is a finding.

Fix: Register all the instant messaging system ports and protocols.

Comments:							
Finding		Not a Finding		Not Reviewed		Not Applicable	

2.7 Vulnerability and Asset Management

IM0460: The instant messaging system is not registered in VMS

Vulnerability Key: V0015466

STIG ID: IM0460

Vulnerability: The instant messaging system is not registered in VMS.

IA Controls: VIVM-1 Vulnerability Management

Categories: 12.5 IAVM Process

Responsibility: Information Assurance Officer / System Administrator

References: Instant Messaging STIG

Severity: Category II

Vulnerability Discussion: Running the most current, approved version of software on all instant messaging servers will help maintain a stable base of security fixes as well as security enhancements. Instant messaging servers that are not running the latest tested and approved versions of software are vulnerable to the potential attacks. Furthermore, if the instant messaging server is no longer supported by the vendor, patches will not be made available to address weaknesses exposing new vulnerabilities, nor will IAVM notices be made available that provide announcements of these new vulnerabilities along with measures to mitigate their associated risks.

Computing Check: Review the instant messaging system assets in VMS. If they are not registered, then this is a finding.

Fix: Register the instant messaging system in VMS.

Comments:							
Finding		Not a Finding		Not Reviewed		Not Applicable	

2.8 Product Specific Checklists

IM0470: Instant messaging system is not configured to product specific checklist

Vulnerability Key: V0015467

STIG ID: IM0470

Vulnerability: Instant messaging system is not configured to product specific checklist.

IA Controls: ECSC-1 Security Configuration Compliance

Categories: 12.4 CM Process

Responsibility: Information Assurance Officer / System Administrator

References: Instant Messaging STIG

Severity: Category II

Vulnerability Discussion: There are specific product dependent settings and controls that will need to be configured to ensure the secure configuration of the instant messaging systems. Because these controls do not apply to every instant messaging product, the specifics are documented in the associated product specific companion checklist. Without these settings configured, instant messaging systems may have many vulnerabilities open.

Computing Check: Request a copy of the specific instant messaging checklist used to configure the instant messaging system. If the checklist was not used to configure the system, then this is a finding. If no product specific checklist exists for the product, then this is not applicable.

Fix: Use the product specific checklist to configure the instant messaging system.

Comments:							
Finding		Not a Finding		Not Reviewed		Not Applicable	

2.9 Instant Messaging

IM0500: No antivirus software is installed on IM clients computers

Vulnerability Key: V0015468

STIG ID: IM0500

Vulnerability: No antivirus software is installed on instant messaging client computers.

IA Controls: ECVP-1 Virus Protection

Categories: 14.7 Antivirus

Responsibility: Information Assurance Officer / System Administrator

References: Instant Messaging STIG

Severity: Category I

Vulnerability Discussion: Malicious Software (Malware) is any program or file that is harmful to a computer. Malware includes computer viruses, worms, Trojan horses, and spyware. Malware has the capability to corrupt files, alter or delete data, distribute confidential data, disable hardware, deny legitimate user access, and cause hard drives to crash. Malware is also able to send itself from an email account or IM buddy list to all of a user’s contacts. IM is a potential carrier for Malware because it provides the ability to transfer text messages and files. This means that IM can transfer Malware and provide an access point for a backdoor Trojan horse to gain access to a computer without opening a listening port (TCP/UDP) and bypassing most desktop firewall controls. Once connected to the computer, the Malware is able to utilize the buddy list to infect other users.

Computing Check: Review IM client computers to verify antivirus software has been installed. For windows operating systems, go to start, control panel, and add/remove programs. Review the installed programs looking for antivirus software (Mcafee, Symantec, or Trend Micro are JTF-GNO approved). If no antivirus software is installed, then this is a finding.

Fix: Install antivirus software on all IM client computers.

Comments:							
Finding		Not a Finding		Not Reviewed		Not Applicable	

IM0510: IM community announcements are not restricted to authorized users only

Vulnerability Key: V0015469

STIG ID: IM0510

Vulnerability: IM community announcements are not restricted to authorized users only.

IA Controls: ECSC-1 Security Configuration Compliance

Categories: 12.4 CM Process

Responsibility: Information Assurance Officer / System Administrator

References: Instant Messaging STIG

Severity: Category II

Vulnerability Discussion: Restricting IM chat announcements to only authorized users limit attackers from connecting to computers on the network and sending malicious code.

Computing Check: Review the IM server configuration to verify chat announcements are disabled or restricted to specific users. If chat announcements are enabled for all users, then this is a finding.

Fix: Configure IM chat announcements to authorized users only.

Comments:							
Finding		Not a Finding		Not Reviewed		Not Applicable	

IM0520: No policy prohibiting IM file sharing exists

Vulnerability Key: V0015470

STIG ID: IM0520

Vulnerability: No policy prohibiting IM file sharing exists.

IA Controls: ECSC-1 Security Configuration Compliance

Categories: 12.4 CM Process

Responsibility: Information Assurance Officer / System Administrator

References: Instant Messaging STIG

Severity: Category III

Vulnerability Discussion: IM provides file-sharing capabilities, which is used to access files on remote computers via a screen name. The screen name will probably never change, so infecting the computer with malware is not difficult. Once the computer becomes infected with a Trojan horse, tracking the infected computer is rather easy. Furthermore, the attacker does not need to open a new suspicious port for communication. The attacker may use the open instant messaging ports. There are a handful of Trojan horse programs that target instant messaging. Some modify configuration settings so file sharing is enabled for the entire hard drive. These types of Trojan horses pose a large threat, as they allow anyone full file access to the computer.

Non-Computing Check: Request a copy of the IM policy prohibiting file sharing. If no policy can be produced, then this is a finding.

Fix: Create a policy prohibiting IM file sharing.

Comments:							
Finding		Not a Finding		Not Reviewed		Not Applicable	

IM0530: IM file sharing is enabled

Vulnerability Key: V0015471

STIG ID: IM0530

Vulnerability: IM file sharing is enabled.

IA Controls: ECSC-1 Security Configuration Compliance

Categories: 12.4 CM Process

Responsibility: Information Assurance Officer / System Administrator

References: Instant Messaging STIG

Severity: Category II

Vulnerability Discussion: IM provides file-sharing capabilities, which is used to access files on remote computers via a screen name. The screen name will probably never change, so infecting the computer with malware is not difficult. Once the computer becomes infected with a Trojan horse, tracking the infected computer is rather easy. Furthermore, the attacker does not need to open a new suspicious port for communication. The attacker may use the open instant messaging ports. There are a handful of Trojan horse programs that target instant messaging. Some modify configuration settings so file sharing is enabled for the entire hard drive. These types of Trojan horses pose a large threat, as they allow anyone full file access to the computer.

Computing Check: Review the server and client configurations to determine if file sharing is disabled. Work with the system administrator to review these configurations. If file sharing is enabled, then this is a finding.

Fix: Disable all IM file sharing capabilities**.**

Comments:							
Finding		Not a Finding		Not Reviewed		Not Applicable	

IM0560: IM server ports are open that are not required for operation

Vulnerability Key: V0015472

STIG ID: IM0560

Vulnerability: IM server ports are open that are not required for operation. Ports that are required for operation are not documented with the IAO/SA.

IA Controls: ECSC-1 Security Configuration Compliance

Categories: 12.4 CM Process

Responsibility: Information Assurance Officer / System Administrator

References: Instant Messaging STIG

Severity: Category II

Vulnerability Discussion: Open IM server ports may be used by attackers to find potential vulnerabilities on the server operation system, applications, or databases. Only ports required for IM operation should be open minimizing the risk of external scans and attacks.

Computing Check: Review the IM server configuration and compare the ports open for the IM server to the documented IM ports. If IM ports are open that are not documented, then this is a finding.

Fix: Disable all ports not required for IM server operation.

Comments:

Finding		Not a Finding		Not Reviewed		Not Applicable	

IM0570: Unapproved IM client software used

Vulnerability Key: V0015473

STIG ID: IM0570

Vulnerability: Unapproved IM client software used on IM network. Approved IM client software is not documented with the IAO/SA.

IA Controls: ECSC-1 Security Configuration Compliance, DCPR-1 CM Process

Categories: 12.4 CM Process

Responsibility: Information Assurance Officer / System Administrator

References: Instant Messaging STIG

Severity: Category II

Vulnerability Discussion: A very large number of freeware/shareware IM clients exist, many of which could be highly vulnerable to attack or subversion. Unless otherwise configured, the IM server can accept connection from any compliant client. Potential problems could occur if the IM server permits connections from non-vendor-supported clients.

Computing Check: Review the IM client software used on the IM network. Compare this with the documented IM client software that has been approved for use. If IM client software is used on the network that is not documented, then this is a finding.

Fix: Utilize only approved IM client software.

Comments:

Finding		Not a Finding		Not Reviewed		Not Applicable	

IM0580: Common IM domain names are not blocked

Vulnerability Key: V0015474

STIG ID: IM0580

Vulnerability: Common IM domain names are not blocked at enclave perimeter.

IA Controls: ECSC-1 Security Configuration Compliance

Categories: 4.1 Unneeded Ports, Protocols, and Services

Responsibility: Information Assurance Officer / System Administrator

References: Instant Messaging STIG

Severity: Category II

Vulnerability Discussion: IM traffic frequently connects to commonly allowed destination ports such as HTTP. If the standard IM ports are blocked, IM clients will attempt to connect on common destination ports such as Telnet, FTP, SMTP, etc. If the client is unable to access the IM server via a common destination port due to protocol analysis, IM traffic can instead be tunneled via HTTP. Tunneled IM packets are embedded into an HTTP POST request and bypass firewalls. To block this type of traffic, you must block the domain names or IP addresses.

Computing Check: Work with the network reviewer and system administrator to review the enclave firewall and proxy server perimeter configuration. Verify that the following IM domain names or IP addresses are blocked OUTBOUND and INBOUND at the firewall or proxy. Verify the following domain names are denied OUTBOUND and INBOUND access through the proxy server or firewall:

- AOL Instant Messenger: **login.oscar.aol.com:443**, **aimexpress.oscar.aol.com**
- AOL Instant Messenger: **login.oscar.aol.com, possibly toc.oscar.aol.com and login.icq.com**
- ICQ: **login.icq.com** and **http.proxy.icq.com** (Was icq.mirabilis.com and login.icq.com previously)
- MSN Messenger: **messenger.hotmail.com, gateway.messenger.hotmail.com, login.net.passport.com**
- Yahoo! IM: scs.msg.yahoo.com, scsb.msg.yahoo.com, scsc.msg.yahoo.com, scs.yahoo.com, and shttp.msg.yahoo.com
- Yahoo! Messenger: **msg.edit.yahoo.com/***, **messenger.yahoo.com/*,** and **http.pager.yahoo.com/***.

Fix: Block the instant messaging domain names at the enclave proxy server or firewall.

Comments:

Finding		Not a Finding		Not Reviewed		Not Applicable	

IM0590: No IM user policy behavior policy exists

Vulnerability Key: V0015475

STIG ID: IM0590

Vulnerability: No IM user policy exists outlining the acceptable behavior and consequences for violation of the policy.

IA Controls: PRRB-1 Security Rules of Behavior or Acceptable Use Policy

Categories: 6.4 Training & Certification

Responsibility: Information Assurance Officer / System Administrator

References: Instant Messaging STIG

Severity: Category III

Vulnerability Discussion: IM in the enterprise poses the risk of information disclosure to unauthorized users. Within any instant messaging environment there is the potential to disclose information proprietary or sensitive in nature. The risk for disclosure of classified or aggregated information is also possible. These risks must be addressed within the user community by implementing user policies to ensure users are aware of acceptable behavior during IM interactions.

Non-Computing Check: Request a copy of the IM user behavior policy from the IAO/SA. If no policy can be produced, then this is a finding.

Fix: Create an acceptable user behavior policy for instant messaging usage.

Comments:							
Finding		Not a Finding		Not Reviewed		Not Applicable	

IM0600: No IM instruction presented to users to mitigate IM risks

Vulnerability Key: V0015476

STIG ID: IM0600

Vulnerability: No IM instruction presented to all users outlining known IM risks and possible ways to mitigate these risks.

IA Controls: PRTN-1 Information Assurance Training

Categories: 6.4 Training & Certification

Responsibility: Information Assurance Officer / System Administrator

References: Instant Messaging STIG

Severity: Category III

Vulnerability Discussion: There is no such thing as a risk-free IM environment. Implementing a strategic IM management program that combines written policy with education and enforcement, organizations can mitigate IM disasters, IM misuse, and limit costly liabilities.

Non-Computing Check: Request a copy of the IM guidance from the IAO/SA presented to all IM users. The IM guidance must include the following at a minimum:

- Do not respond to users that you do not know
- Keep your password private and change it at regular intervals
- Do not send classified or sensitive data over IM
- Do not download or install public IM clients on DoD computers
- IM communication will be monitored
- Do not send files over IM

Fix: Provide IM instruction to all users.

Comments:							
Finding		Not a Finding		Not Reviewed		Not Applicable	

2.10 Virtual Meetings

The following checks apply to instant messaging systems that provide the capability to host virtual meetings. Most IM enterprise systems provide virtual meeting capabilities. Work with the system administrator and review the vendor's website to review the features of the instant messaging system to determine if these requirements apply.

IM0700: Virtual spaces or rooms are not restricted to authorized users

Vulnerability Key: V0015477

STIG ID: IM0700

Vulnerability: Virtual spaces or rooms are not restricted to authorized users.

IA Controls: ECCD-1 Changes to Data

Categories: 2.1 Object Permissions

Responsibility: Information Assurance Officer / System Administrator

References: Instant Messaging STIG

Severity: Category II

Vulnerability Discussion: Virtual meetings are typically conducted in virtual spaces and rooms. Virtual areas must have owners and access controls, otherwise users will be able to move throughout the virtual areas unrestricted. This type of access allows users to access data and files that maybe sensitive or classified. This may result in data theft or unauthorized users viewing data.

Computing Check: Review the access control configuration for virtual spaces and rooms. Verify that users are restricted based on function and role. If no type of access control is configured, then this is a finding.

Fix: Implement access controls for all users for all virtual areas.

Comments:							
Finding		Not a Finding		Not Reviewed		Not Applicable	

IM0710: Virtual spaces and rooms are not labeled according to classification

Vulnerability Key: V0015478

STIG ID: IM0710

Vulnerability: Virtual spaces and rooms are not labeled according to the classification assignment (unclassified, FOUO, classified).

IA Controls: ECAN-1 Access for Need-to-Know

Categories: 11.1 Marking

Responsibility: Information Assurance Officer / System Administrator

References: Instant Messaging STIG

Severity: Category II

Vulnerability Discussion: Virtual meetings will have data classifications that follow the confidentiality controls of the DoD. Virtual meetings can have many room types such as Open, Secret, Members Only, Password Protected, and Invitation Only. Care must be taken so that sensitive information is not disclosed to unauthorized persons. Sharing sensitive information should be done in a closed community. Open rooms will not be used for meetings that contain sensitive DoD information. Virtual meetings will have data labeled as unclassified, unclassified FOUO, or classified. Virtual meetings will be configured to enforce classification levels for all network shared applications and data.

Computing Check: Review the labeling of the virtual spaces or rooms. Ensure the labeling exists and matches the appropriate classification. If no labeling exists or labeling is inaccurate, then this is a finding.

Fix: Label all virtual spaces with the appropriate classification label.

Comments:							
Finding		Not a Finding		Not Reviewed		Not Applicable	

IM0720: Virtual meeting data is not labeled in accordance to the classification of the virtual area

Vulnerability Key: V0015479

STIG ID: IM0720

Vulnerability: Virtual meeting data is not labeled in accordance to the classification of the virtual space or room (unclassified, FOUO, or classified).

IA Controls: ECAN-1 Access for Need-to-Know

Categories: 11.1 Marking

Responsibility: Information Assurance Officer / System Administrator

References: Instant Messaging STIG

Severity: Category II

Vulnerability Discussion: Virtual meetings will have data classifications that follow the confidentiality controls of the DoD. Virtual meetings can have many room types such as Open, Secret, Members Only, Password Protected, and Invitation Only. Care must be taken so that sensitive information is not disclosed to unauthorized persons. Sharing sensitive information should be done in a closed community. Open rooms will not be used for meetings that contain sensitive DoD information. Virtual meetings will have data labeled as unclassified, unclassified FOUO, or classified. Virtual meetings will be configured to enforce classification levels for all network shared applications and data.

Computing Check: Ask the IAO/SA if the data for virtual meetings is labeled according to the classification assignment. Data that could be labeled includes whiteboard contents, word documents, file cabinet contents, etc. If no classification for data exists, then this is a finding.

Fix: Label all data for virtual meetings.

Comments:							
Finding		Not a Finding		Not Reviewed		Not Applicable	

IM0730: Virtual meetings tools are not disabled if not required for virtual meeting

Vulnerability Key: V0015480

STIG ID: IM0730

Vulnerability: Virtual meeting tools are not disabled if not required for virtual meeting.

IA Controls: ECSC-1 Security Configuration Compliance

Categories: 2.1 Object Permissions

Responsibility: Information Assurance Officer / System Administrator

References: Instant Messaging STIG

Severity: Category II

Vulnerability Discussion: Only virtual meeting tools required for the virtual meeting should be enabled. Moderators act as the administrator of the virtual meeting. Moderators are able to invite or un-invite users, and modify, add, and delete tools according to meeting requirements. Tools that are available for meetings may be screen sharing, whiteboards, slides, polling, etc.

Computing Check: Check the virtual meeting server and review the tools available for use within virtual meetings. Request the documentation of the virtual meeting tools required for virtual meetings. If no documentation can be produced, then this is a finding.

Fix: Document all virtual meeting tools required for virtual meetings.

Comments:							
Finding		Not a Finding		Not Reviewed		Not Applicable	

IM0740: Uninvited users are able to participate in virtual meetings

Vulnerability Key: V0015481

STIG ID: IM0740

Vulnerability: Uninvited users are able to participate in virtual meetings.

IA Controls: ECSD-1 Software Development Change Controls

Categories: 2.1 Object Permissions

Responsibility: Information Assurance Officer / System Administrator

References: Instant Messaging STIG

Severity: Category II

Vulnerability Discussion: Uninvited users should not be able to participate in virtual meetings. Virtual meetings should be restricted to authorized users only. Uninvited users may be allowed to view or access data and files that maybe sensitive or classified. This may result in data theft or unauthorized users viewing data.

Computing Check: Review the instant messaging server configuration to verify that only invited users may attend virtual meetings. If this is not configured, then this is a finding.

Fix: Configure the instant messaging server to allow only invited users to virtual meetings.

Comments:							
Finding		Not a Finding		Not Reviewed		Not Applicable	

IM0750: Virtual meetings do not require passwords

Vulnerability Key: V0015482

STIG ID: IM0750

Vulnerability: Virtual meetings do not require passwords.

IA Controls: ECSC-1 Security Configuration Compliance

Categories: 1.4 Authentication Services, 2.1 Object Permissions

Responsibility: Information Assurance Officer / System Administrator

References: Instant Messaging STIG

Severity: Category II

Vulnerability Discussion: The meeting password is an additional security feature that provides password protection for individual meetings. The meeting password is different from the user's password required to login to the instant messaging system.

Computing Check: Review the instant messaging server configuration to verify that passwords are required for all virtual meetings. If this is not configured, then this is a finding.

Fix: Configure virtual meetings to require passwords for entry.

Comments:							
Finding		Not a Finding		Not Reviewed		Not Applicable	

IM0800: Virtual meeting application sharing tools are not restricted to authorized users

Vulnerability Key: V0015483

STIG ID: IM0800

Vulnerability: Virtual meeting application sharing tools are not restricted to authorized users.

IA Controls: ECSC-1 Security Configuration Compliance

Categories: 2.1 Object Permissions

Responsibility: Information Assurance Officer / System Administrator

References: Instant Messaging STIG

Severity: Category III

Vulnerability Discussion: Application sharing tools required for the virtual meeting should be restricted to authorized users only. Some products allow users to simultaneously use whiteboards, bulletin boards, and discussion tools. These applications are available to all authorized users within the virtual meeting. Application sharing will be limited to authorized users within the virtual meeting.

Computing Check: Review the user privileges for the application sharing tools on the instant messaging server. Ensure only authorized users may start, open, and use these tools. If unauthorized users are able to access these tools, then this is a finding.

Fix: Restrict application sharing tools to authorized users only.

Comments:

Finding		Not a Finding		Not Reviewed		Not Applicable	

APPENDIX A. FIPS 140-2 APPROVED ALGORITHMS

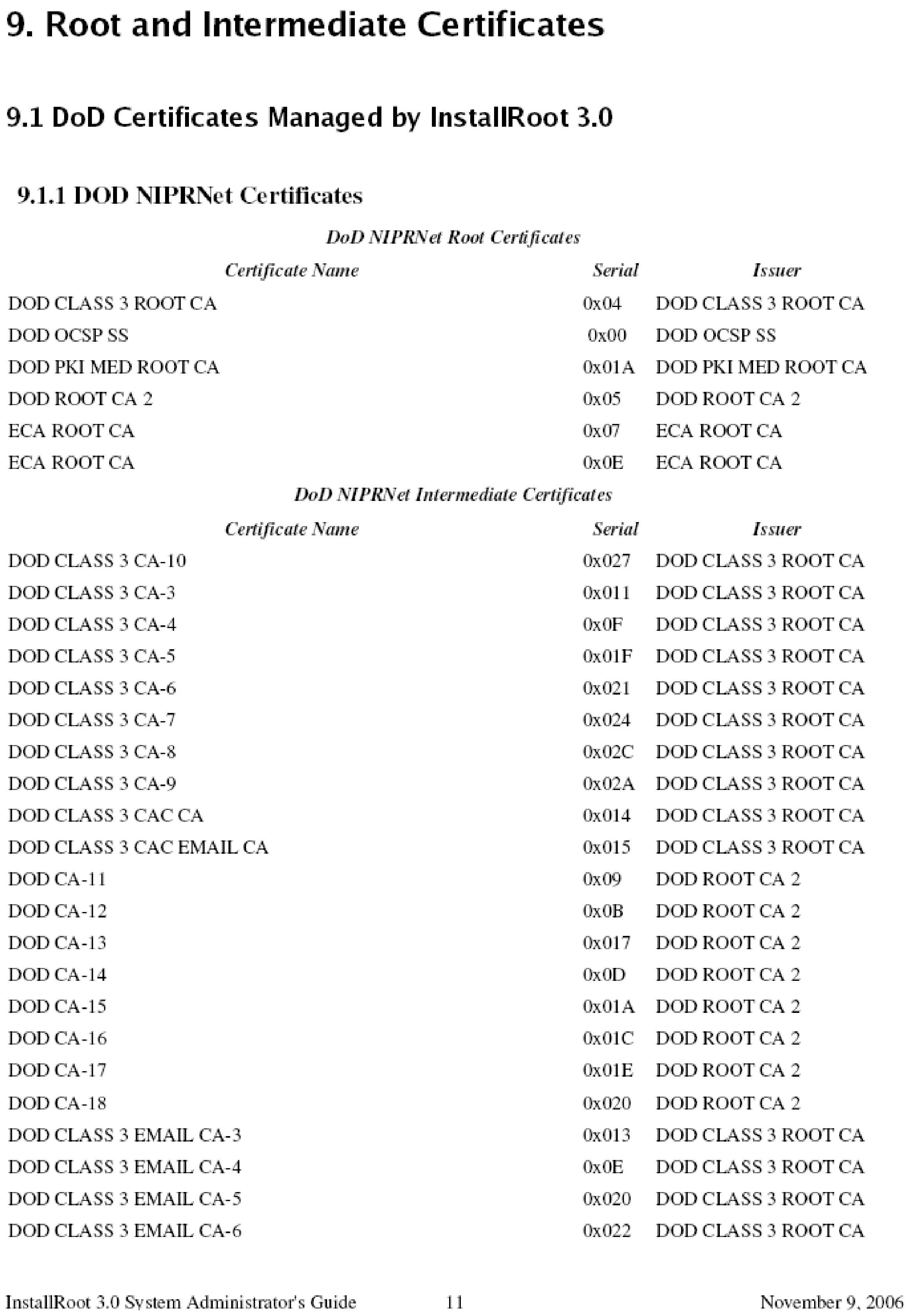
Symmetric Key – Encryption
AES (Advanced Encryption Standard)
3DES (Triple Data Encryption Standard)
SkipJack (Escrowed Encryption Standard)

Asymmetric Key – Signature
DSA (Digital Signature Standard)
RSA
ECDSA (Elliptic Curve Digital Signature Algorithm)

Message Authentication
HMAC (Keyed-Hash Message Authentication Code)
3DES MAC
Recommended Block Cipher Modes:
The CCM Mode for Authentication and Confidentiality
The CMAC Mode for Authentication

Hashing
Secure Hash Standard (SHA-1, SHA-224, SHA-256, SHA-384, and SHA-512)

APPENDIX B. DOD CERTIFICATES



9. Root and Intermediate Certificates

9.1 DoD Certificates Managed by InstallRoot 3.0

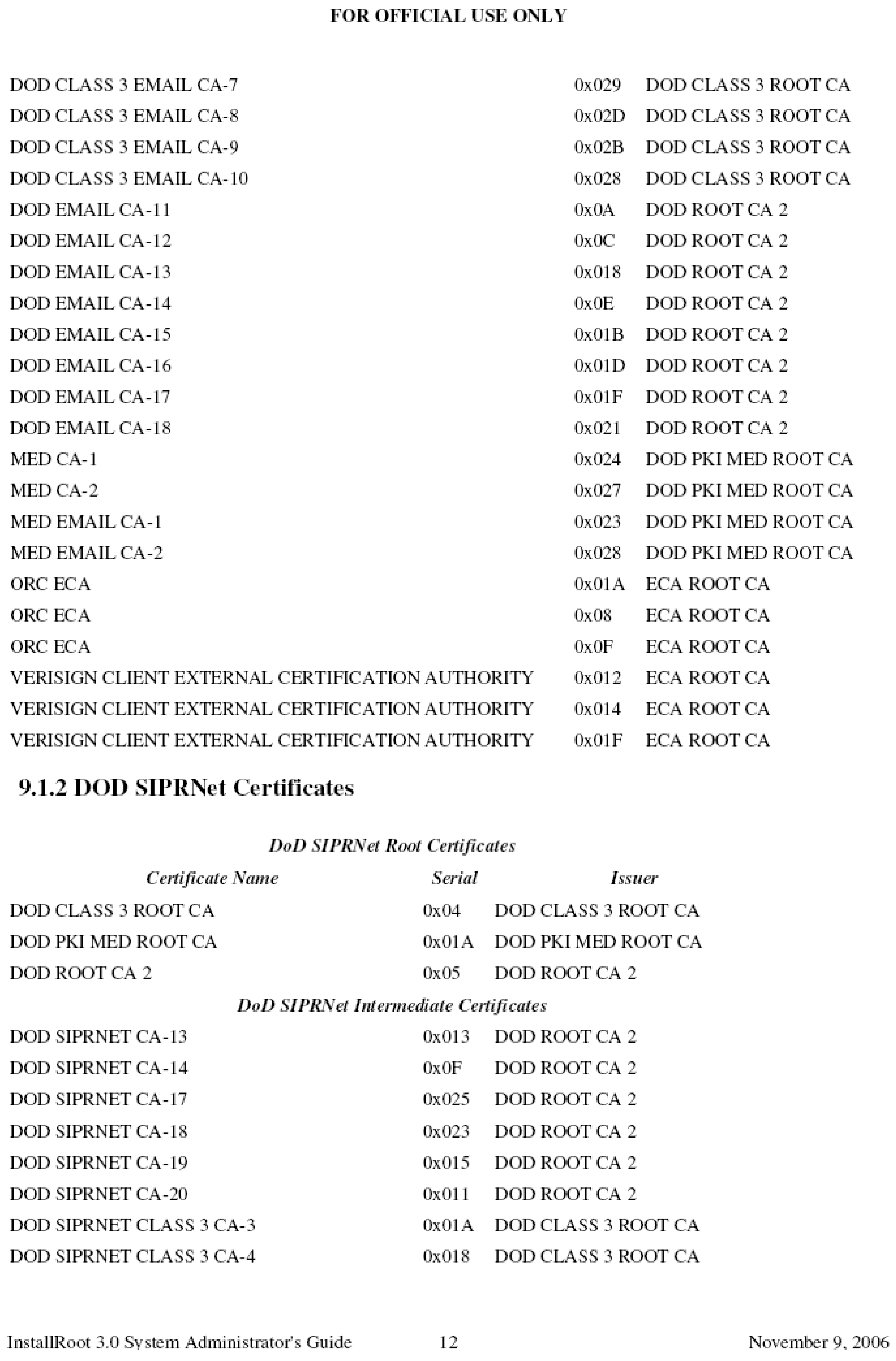
9.1.1 DOD NIPRNet Certificates

DoD NIPRNet Root Certificates

Certificate Name	*Serial*	*Issuer*
DOD CLASS 3 ROOT CA	0x04	DOD CLASS 3 ROOT CA
DOD OCSP SS	0x00	DOD OCSP SS
DOD PKI MED ROOT CA	0x01A	DOD PKI MED ROOT CA
DOD ROOT CA 2	0x05	DOD ROOT CA 2
ECA ROOT CA	0x07	ECA ROOT CA
ECA ROOT CA	0x0E	ECA ROOT CA

DoD NIPRNet Intermediate Certificates

Certificate Name	*Serial*	*Issuer*
DOD CLASS 3 CA-10	0x027	DOD CLASS 3 ROOT CA
DOD CLASS 3 CA-3	0x011	DOD CLASS 3 ROOT CA
DOD CLASS 3 CA-4	0x0F	DOD CLASS 3 ROOT CA
DOD CLASS 3 CA-5	0x01F	DOD CLASS 3 ROOT CA
DOD CLASS 3 CA-6	0x021	DOD CLASS 3 ROOT CA
DOD CLASS 3 CA-7	0x024	DOD CLASS 3 ROOT CA
DOD CLASS 3 CA-8	0x02C	DOD CLASS 3 ROOT CA
DOD CLASS 3 CA-9	0x02A	DOD CLASS 3 ROOT CA
DOD CLASS 3 CAC CA	0x014	DOD CLASS 3 ROOT CA
DOD CLASS 3 CAC EMAIL CA	0x015	DOD CLASS 3 ROOT CA
DOD CA-11	0x09	DOD ROOT CA 2
DOD CA-12	0x0B	DOD ROOT CA 2
DOD CA-13	0x017	DOD ROOT CA 2
DOD CA-14	0x0D	DOD ROOT CA 2
DOD CA-15	0x01A	DOD ROOT CA 2
DOD CA-16	0x01C	DOD ROOT CA 2
DOD CA-17	0x01E	DOD ROOT CA 2
DOD CA-18	0x020	DOD ROOT CA 2
DOD CLASS 3 EMAIL CA-3	0x013	DOD CLASS 3 ROOT CA
DOD CLASS 3 EMAIL CA-4	0x0E	DOD CLASS 3 ROOT CA
DOD CLASS 3 EMAIL CA-5	0x020	DOD CLASS 3 ROOT CA
DOD CLASS 3 EMAIL CA-6	0x022	DOD CLASS 3 ROOT CA



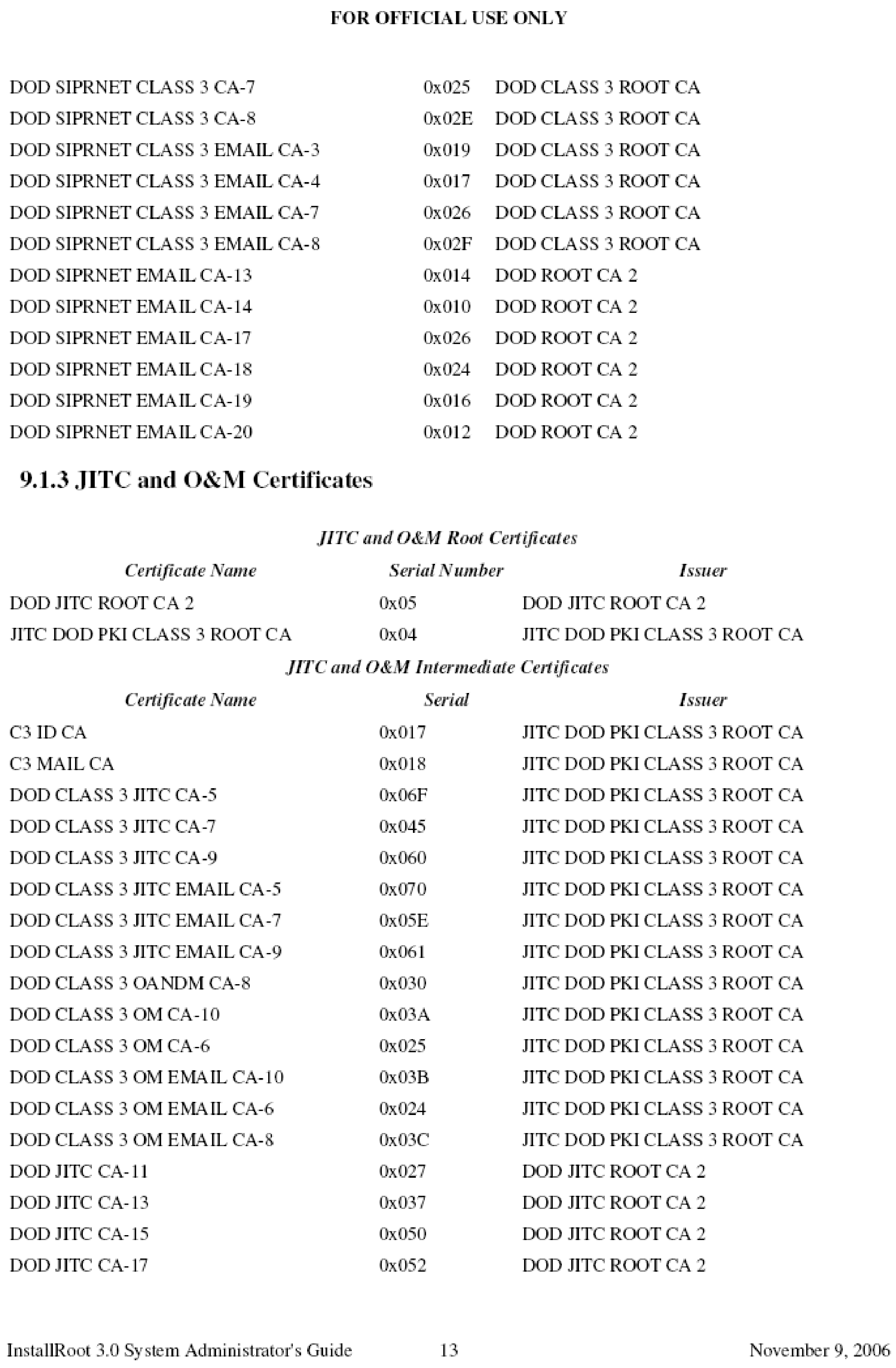
FOR OFFICIAL USE ONLY

DOD CLASS 3 EMAIL CA-7	0x029	DOD CLASS 3 ROOT CA
DOD CLASS 3 EMAIL CA-8	0x02D	DOD CLASS 3 ROOT CA
DOD CLASS 3 EMAIL CA-9	0x02B	DOD CLASS 3 ROOT CA
DOD CLASS 3 EMAIL CA-10	0x028	DOD CLASS 3 ROOT CA
DOD EMAIL CA-11	0x0A	DOD ROOT CA 2
DOD EMAIL CA-12	0x0C	DOD ROOT CA 2
DOD EMAIL CA-13	0x018	DOD ROOT CA 2
DOD EMAIL CA-14	0x0E	DOD ROOT CA 2
DOD EMAIL CA-15	0x01B	DOD ROOT CA 2
DOD EMAIL CA-16	0x01D	DOD ROOT CA 2
DOD EMAIL CA-17	0x01F	DOD ROOT CA 2
DOD EMAIL CA-18	0x021	DOD ROOT CA 2
MED CA-1	0x024	DOD PKI MED ROOT CA
MED CA-2	0x027	DOD PKI MED ROOT CA
MED EMAIL CA-1	0x023	DOD PKI MED ROOT CA
MED EMAIL CA-2	0x028	DOD PKI MED ROOT CA
ORC ECA	0x01A	ECA ROOT CA
ORC ECA	0x08	ECA ROOT CA
ORC ECA	0x0F	ECA ROOT CA
VERISIGN CLIENT EXTERNAL CERTIFICATION AUTHORITY	0x012	ECA ROOT CA
VERISIGN CLIENT EXTERNAL CERTIFICATION AUTHORITY	0x014	ECA ROOT CA
VERISIGN CLIENT EXTERNAL CERTIFICATION AUTHORITY	0x01F	ECA ROOT CA

9.1.2 DOD SIPRNet Certificates

DoD SIPRNet Root Certificates

Certificate Name	*Serial*	*Issuer*
DOD CLASS 3 ROOT CA	0x04	DOD CLASS 3 ROOT CA
DOD PKI MED ROOT CA	0x01A	DOD PKI MED ROOT CA
DOD ROOT CA 2	0x05	DOD ROOT CA 2
DoD SIPRNet Intermediate Certificates		
DOD SIPRNET CA-13	0x013	DOD ROOT CA 2
DOD SIPRNET CA-14	0x0F	DOD ROOT CA 2
DOD SIPRNET CA-17	0x025	DOD ROOT CA 2
DOD SIPRNET CA-18	0x023	DOD ROOT CA 2
DOD SIPRNET CA-19	0x015	DOD ROOT CA 2
DOD SIPRNET CA-20	0x011	DOD ROOT CA 2
DOD SIPRNET CLASS 3 CA-3	0x01A	DOD CLASS 3 ROOT CA
DOD SIPRNET CLASS 3 CA-4	0x018	DOD CLASS 3 ROOT CA



FOR OFFICIAL USE ONLY

DOD SIPRNET CLASS 3 CA-7	0x025	DOD CLASS 3 ROOT CA
DOD SIPRNET CLASS 3 CA-8	0x02E	DOD CLASS 3 ROOT CA
DOD SIPRNET CLASS 3 EMAIL CA-3	0x019	DOD CLASS 3 ROOT CA
DOD SIPRNET CLASS 3 EMAIL CA-4	0x017	DOD CLASS 3 ROOT CA
DOD SIPRNET CLASS 3 EMAIL CA-7	0x026	DOD CLASS 3 ROOT CA
DOD SIPRNET CLASS 3 EMAIL CA-8	0x02F	DOD CLASS 3 ROOT CA
DOD SIPRNET EMAIL CA-13	0x014	DOD ROOT CA 2
DOD SIPRNET EMAIL CA-14	0x010	DOD ROOT CA 2
DOD SIPRNET EMAIL CA-17	0x026	DOD ROOT CA 2
DOD SIPRNET EMAIL CA-18	0x024	DOD ROOT CA 2
DOD SIPRNET EMAIL CA-19	0x016	DOD ROOT CA 2
DOD SIPRNET EMAIL CA-20	0x012	DOD ROOT CA 2

9.1.3 JITC and O&M Certificates

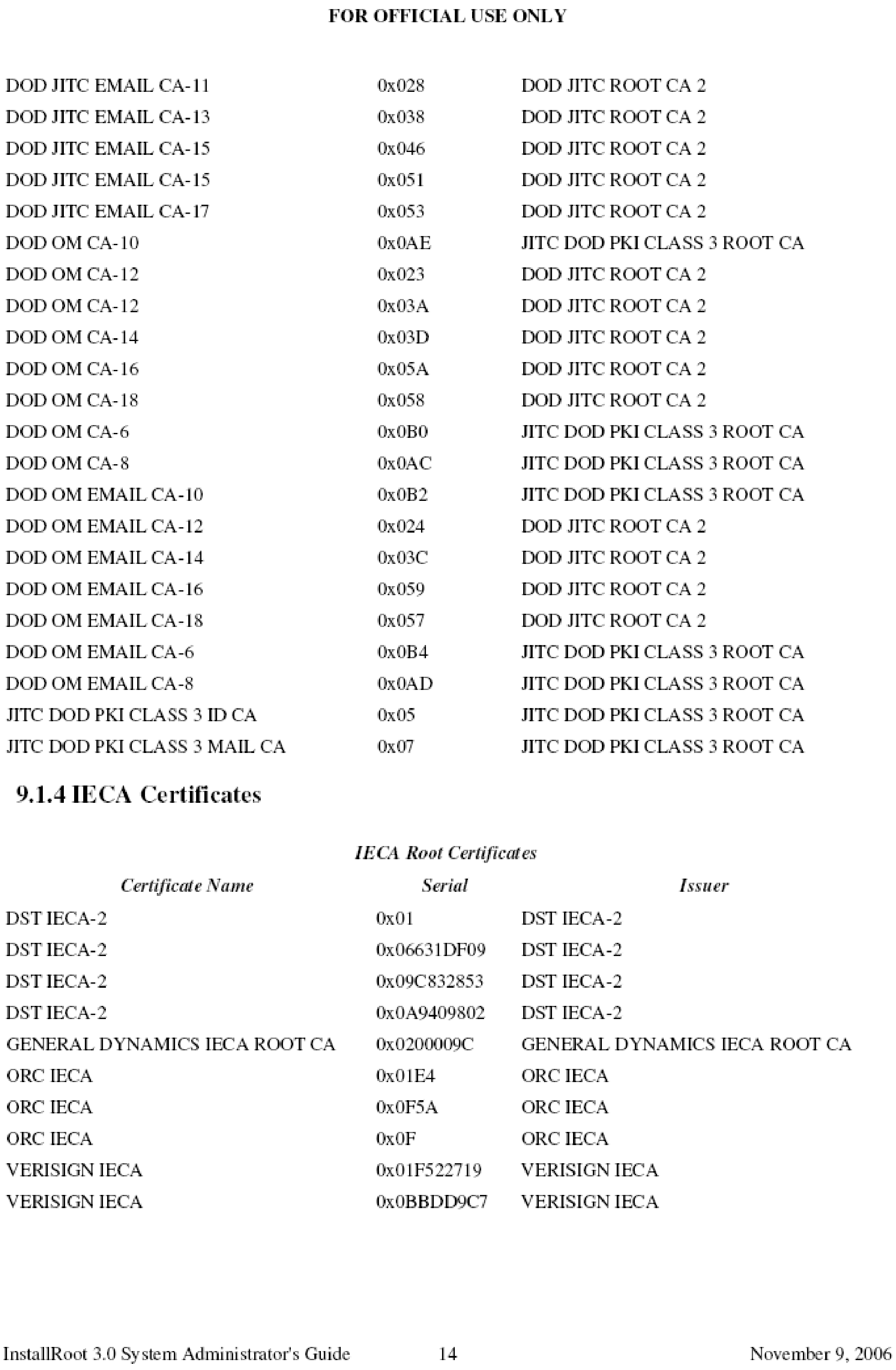
JITC and O&M Root Certificates

Certificate Name	*Serial Number*	*Issuer*
DOD JITC ROOT CA 2	0x05	DOD JITC ROOT CA 2
JITC DOD PKI CLASS 3 ROOT CA	0x04	JITC DOD PKI CLASS 3 ROOT CA

JITC and O&M Intermediate Certificates

Certificate Name	*Serial*	*Issuer*
C3 ID CA	0x017	JITC DOD PKI CLASS 3 ROOT CA
C3 MAIL CA	0x018	JITC DOD PKI CLASS 3 ROOT CA
DOD CLASS 3 JITC CA-5	0x06F	JITC DOD PKI CLASS 3 ROOT CA
DOD CLASS 3 JITC CA-7	0x045	JITC DOD PKI CLASS 3 ROOT CA
DOD CLASS 3 JITC CA-9	0x060	JITC DOD PKI CLASS 3 ROOT CA
DOD CLASS 3 JITC EMAIL CA-5	0x070	JITC DOD PKI CLASS 3 ROOT CA
DOD CLASS 3 JITC EMAIL CA-7	0x05E	JITC DOD PKI CLASS 3 ROOT CA
DOD CLASS 3 JITC EMAIL CA-9	0x061	JITC DOD PKI CLASS 3 ROOT CA
DOD CLASS 3 OANDM CA-8	0x030	JITC DOD PKI CLASS 3 ROOT CA
DOD CLASS 3 OM CA-10	0x03A	JITC DOD PKI CLASS 3 ROOT CA
DOD CLASS 3 OM CA-6	0x025	JITC DOD PKI CLASS 3 ROOT CA
DOD CLASS 3 OM EMAIL CA-10	0x03B	JITC DOD PKI CLASS 3 ROOT CA
DOD CLASS 3 OM EMAIL CA-6	0x024	JITC DOD PKI CLASS 3 ROOT CA
DOD CLASS 3 OM EMAIL CA-8	0x03C	JITC DOD PKI CLASS 3 ROOT CA
DOD JITC CA-11	0x027	DOD JITC ROOT CA 2
DOD JITC CA-13	0x037	DOD JITC ROOT CA 2
DOD JITC CA-15	0x050	DOD JITC ROOT CA 2
DOD JITC CA-17	0x052	DOD JITC ROOT CA 2

InstallRoot 3.0 System Administrator's Guide	13	November 9, 2006



FOR OFFICIAL USE ONLY

DOD JITC EMAIL CA-11	0x028	DOD JITC ROOT CA 2
DOD JITC EMAIL CA-13	0x038	DOD JITC ROOT CA 2
DOD JITC EMAIL CA-15	0x046	DOD JITC ROOT CA 2
DOD JITC EMAIL CA-15	0x051	DOD JITC ROOT CA 2
DOD JITC EMAIL CA-17	0x053	DOD JITC ROOT CA 2
DOD OM CA-10	0x0AE	JITC DOD PKI CLASS 3 ROOT CA
DOD OM CA-12	0x023	DOD JITC ROOT CA 2
DOD OM CA-12	0x03A	DOD JITC ROOT CA 2
DOD OM CA-14	0x03D	DOD JITC ROOT CA 2
DOD OM CA-16	0x05A	DOD JITC ROOT CA 2
DOD OM CA-18	0x058	DOD JITC ROOT CA 2
DOD OM CA-6	0x0B0	JITC DOD PKI CLASS 3 ROOT CA
DOD OM CA-8	0x0AC	JITC DOD PKI CLASS 3 ROOT CA
DOD OM EMAIL CA-10	0x0B2	JITC DOD PKI CLASS 3 ROOT CA
DOD OM EMAIL CA-12	0x024	DOD JITC ROOT CA 2
DOD OM EMAIL CA-14	0x03C	DOD JITC ROOT CA 2
DOD OM EMAIL CA-16	0x059	DOD JITC ROOT CA 2
DOD OM EMAIL CA-18	0x057	DOD JITC ROOT CA 2
DOD OM EMAIL CA-6	0x0B4	JITC DOD PKI CLASS 3 ROOT CA
DOD OM EMAIL CA-8	0x0AD	JITC DOD PKI CLASS 3 ROOT CA
JITC DOD PKI CLASS 3 ID CA	0x05	JITC DOD PKI CLASS 3 ROOT CA
JITC DOD PKI CLASS 3 MAIL CA	0x07	JITC DOD PKI CLASS 3 ROOT CA

9.1.4 IECA Certificates

IECA Root Certificates

Certificate Name	*Serial*	*Issuer*
DST IECA-2	0x01	DST IECA-2
DST IECA-2	0x06631DF09	DST IECA-2
DST IECA-2	0x09C832853	DST IECA-2
DST IECA-2	0x0A9409802	DST IECA-2
GENERAL DYNAMICS IECA ROOT CA	0x0200009C	GENERAL DYNAMICS IECA ROOT CA
ORC IECA	0x01E4	ORC IECA
ORC IECA	0x0F5A	ORC IECA
ORC IECA	0x0F	ORC IECA
VERISIGN IECA	0x01F522719	VERISIGN IECA
VERISIGN IECA	0x0BBDD9C7	VERISIGN IECA

InstallRoot 3.0 System Administrator's Guide 14 November 9, 2006